Innominate mGuard smart

User's Manual

Software-Release 3.1.0

Innominate Security Technologies AG
Albert-Einstein-Str. 14
12489 Berlin
Germany
Tel.: +49 (0)800-366 4666
info@innominate.com
www.innominate.com

© Innominate Security Technologies AG

December 2005
“Innominate” and “mGuard” are registered trade names of Innominate Security Technologies AG. The mGuard technology is protected by Patent No. 10138865 and 10305413, which were granted by the German Patent Office. Additional patents are pending.
This document may not be copied or transferred in whole or in part without prior written approval.
Innominate AG reserves the right to modify this document at any time without notice. Innominate provides no warranty for the contents of this document. This disclaimer shall also apply to any implicit warranty of marketability or suitability for a specific purpose.
Furthermore, Innominate assumes no liability for errors in this manual or for accidental or consequential damages in connection with the delivery, performance or utilization of this document.
This manual may not be photocopied, duplicated or translated into another language in whole or in part without the prior written approval of Innominate Security Technologies AG.

Innominate Document Number: 553109-168

Table of Contents

1 Introduction 4
Network features 4
Firewall features 4
Anti-Virus features 4
VPN features 4
Additional features 5
Support 5
2 Typical application scenarios 6
Stealth Mode 6
Network Router 6
DMZ 6
VPN Gateway 7
WLAN over VPN 7
3 Control and LEDs 9
4 Startup 10
4.1 Package contents 10
Included in the package 10
4.2 Connect the device 11
5 Configuration 12
Prerequisites 12
5.1 Local Configuration: At startup 12
With a configured network interface 12
Without a configured network interface 12
5.2 Setting Up a Local Configuration Connection 14
Web-based Administrator interface 14
After a connection has been successfully setup 15
Configuring the device 15
5.3 Remote Configuration 16
Prerequisite 16
Performing a remote configuration 16
5.4 Working with tables 16
Insert row 16
Move rows 16
Delete rows 17
5.5 Entry Page 17
5.6 Network Menu 18
Network → Base 18
Network → Stealth 21
Network → Router 22
Network → PPPoE 23
Network → PPTP 23
Network → MAU Configuration (mGuard smart enterprise only) 24
Network → Extended Settings 25
Network → Status 25
5.7 Firewall Menu 27
Firewall → Incoming 27
Firewall → Outgoing 28
Firewall → Port Forwarding 29
Firewall → NAT 30
Firewall → 1:1 NAT 31
Firewall → MAC Filtering 32
Firewall → Extended Settings 33

Firewall → Logs ... 34
5.8 Anti-Virus - Menu ... 35
Kaspersky Engine ... 35
Supported compression formats ... 35
Prerequisites for use ... 35
Anti-Virus License expiration ... 35
File size - limiting ... 35
Anti-Virus → SMTP Options ... 36
Anti-Virus → POP3 Options ... 38
Anti-Virus → HTTP Options ... 40
Anti-Virus → FTP Options ... 43
Anti-Virus → Database Update ... 45
Anti-Virus → Anti-Virus Status ... 46
Anti-Virus → License Request ... 47
Anti-Virus →Install license ... 47
Anti-Virus → Anti-Virus Logs ... 47
Anti-Virus → Anti-Virus Logs ... 49
5.9 VPN Menu ... 50
VPN → Connections ... 50
More IKE Options ... 56
VPN → Machine Certificate ... 58
VPN → L2TP (mGuard smart enterprise only) ... 59
VPN → IPsec Status ... 60
VPN → L2TP Status (mGuard smart enterprise only) ... 61
VPN → VPN Logs ... 61
5.10 Services Menu ... 62
Services → DNS ... 62
Services → DynDNS Monitoring ... 63
Services → DynDNS Registration ... 63
Services → DHCP Intern/Extern ... 64
Services → LLDP (mGuard smart enterprise only) ... 67
Services → Redundancy (mGuard enterprise XL only) ... 67
Services → Remote Logging (mGuard enterprise only) ... 69
Services → SNMP Traps (mGuard enterprise only) ... 70
5.11 Access Menu ... 71
Access → Passwords ... 71
Access → Language ... 72
Access → HTTPS ... 72
Access → SSH ... 73
Access → SNMP (mGuard enterprise only) ... 75
Access → Serial Port/Modem ... 77
5.12 Features Menu ... 79
Features → Local Update ... 79
Features → Online Update ... 79
Features → Install Licenses ... 80
Features → Software Information ... 80
Features → License Information ... 81
Features → Hardware Information ... 81
5.13 Support Menu ... 82
Support → Snapshot ... 82
Support → Status ... 82
5.14 System Menu ... 84
Services → System Time ... 84
System → Configuration Profiles ... 85

Table of Contents

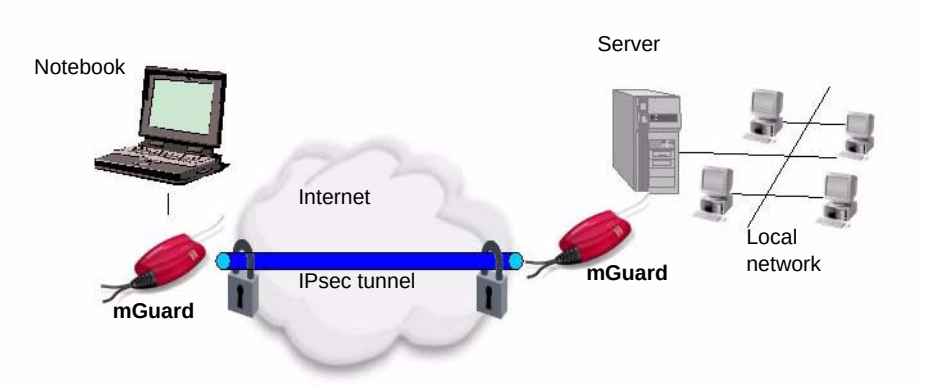
System → Configuration Pull 86
System → Reboot 87
System → Logs 87
5.15 CIDR (Classless InterDomain Routing) 89
5.16 Network Sketch 90
6 The Rescue Button – restart, recovery procedure and to flash the firmware 91
6.1 Performing a Restart 91
6.2 Performing a Recovery 91
6.3 Flashing the firmware 91
Required before the firmware can be flashed: DHCP and TFTP servers 92
6.3.1 Installing DHCP and TFTP servers under Windows or Linux 93
Under Windows: 93
Under Linux 94
7 Glossary 95
Asymmetrical encryption 95
DES / 3DES 95
AES 95
Client / Server 95
Datagram 95
DynDNS provider 96
IP address 96
IPsec 98
NAT (Network Address Translation) 98
Port Number 98
PPPoE 98
PPTP 98
X.509 Certificate 98
Protocol, communication protocol 99
Service Provider 99
Spoofing, Antispoofing 99
Symmetrical encryption 99
TCP/IP (Transmission Control Protocol/Internet Protocol) 99
VLAN 100
VPN (Virtual Private Network) 100
8 Technical data 101

1 Introduction

The mGuard smart protects IP data connections. The device supports the following functions:

- VPN router (VPN - **V**irtual **P**rivate **N**etwork) for the secure transfer of data via public networks (hardware-based DES, 3DES and AES encryption, IPsec protocol)
- Configurable firewall to provide protection against unauthorized access. The dynamic packet filter inspects the source and destination addresses of data packets and blocks undesired traffic.
- Kaspersky virus protection with support for the protocols HTTP, SMTP and POP3.

The device can be conveniently configured using a Web browser.



Network features

- Stealth (Auto, Static, Multi), Router (Static, DHCP Client), PPPoE (for DSL) and PPTP (for DSL) connectivity
- VLAN
- DHCP server/relay on the external and internal network interfaces
- DNS cache on the internal network interface
- Administration using HTTPS and SSH

Firewall features

- Stateful packet inspection
- Anti-spoofing
- IP Filtering
- L2 Filtering (only stealth mode)
- NAT with FTP, IRC and PPTP pass through (only router modes)
- 1:1 NAT (only router modes)
- Port forwarding (only router modes)
- Firewall throughput max. 99MBit/s

Anti-Virus features

- Kaspersky virus protection
- Supported protocols: HTTP, FTP, POP3 and SMTP (sending)

VPN features

- Protocol: IPsec (Tunnel and Transport Mode)
- IPsec DES encryption - 56 Bit
- IPsec 3DES encryption - 168 Bit
- IPsec AES encryption - 128, 192 and 256 Bit
- Packet authentication: MD5, SHA-1
- Internet Key Exchange (IKE) with Main and Quick Mode
- Authentication: Pre-Shared Key (PSK), X.509v3 certificate
- DynDNS
- NAT-T
- Dead Peer Detection (DPD)
- Hardware encryption

- up to 250 VPN tunnels (please refer to the feature table)
- VPN throughput max. 35MBits/s on 266MHz or 70MBit/s on 533MHz models.

Additional features

- MAU management
- Remote logging
- Router/Firewall Redundancy
- IPsec/L2TP Server
- LLDP
- Administration by SNMP v1-v3 (please refer to the feature table) and Innominate Security Configuration Manager (ISCM)

The following table provides an overview which features are available for a specific mGuard model and licence:

		Licence				
		professional		enterprise FW	enterprise	enterprise XL
Model	smart	X	X		X	X
	pci		X		X	X
	delta		X		X	X
	industrial			X		X
	blade				X	X
Hardware	MHz	266	266	533	266	533
	RAM	64	64	64	64	64
	Flash	16	16	16	16	16
Features	VPN Tunnels	2			10	250
	IPsec/L2TP Server				X	X
	MAU Management		X	X	X	X
	Remote Logging		X	X	X	X
	SNMP		X	X	X	X
	LLDP		X	X	X	X
	Redundancy			X		X

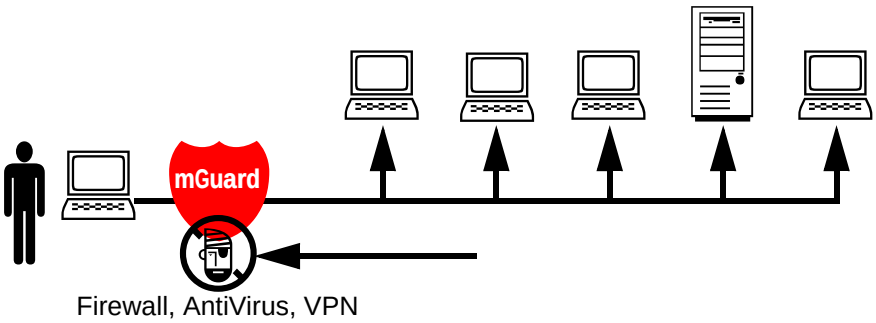
Support

In case of problems with the mGuard please contact your local dealer.
Additional information about the device and relevant changes as well as release notes and software updates can be found on our web site:
http://www.innominate.com/

2 Typical application scenarios

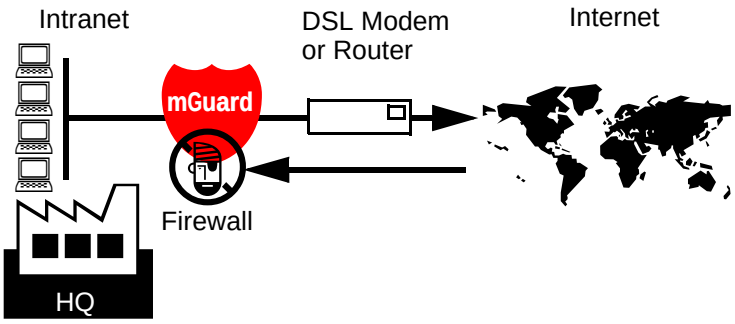
Some of the more common application scenarios may be found below.

Stealth Mode



In *Stealth* Mode (factory default) the mGuard can be installed between an individual computer and the rest of the network.
The settings for Firewall, AntiVirus and VPN can be made with a webbrowser at the URL https://1.1.1.1/.
On the computer itself no configuration changes are required.

Network Router

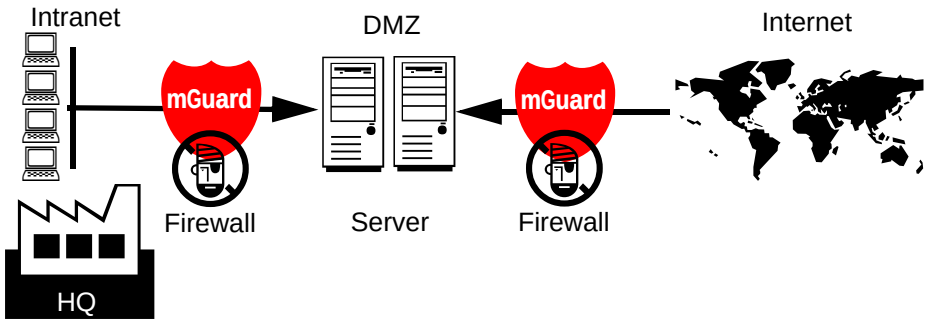


The mGuard is able to provide internet connectivity to a group of computers while protecting the company network with its firewall.
For this purpose one of the following network modes may be used:

- *Router*, if the Internet access is established via a DSL router or dedicated line.
- *PPPoE*, if for example the Internet access is established via a DSL modem using the PPPoE protocol (e.g. in Germany).
- *PPTP*, if for example the Internet access is established via a DSL modem using the PPTP protocol (e.g. in Austria).

The mGuard must be set as the default gateway on the locally connected client system(s).

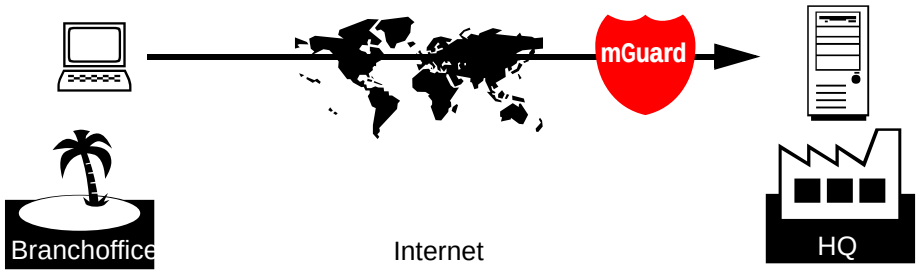
DMZ



A DMZ (Demilitarized Zone) is a protected network, which sits between an internal network and an external network. For example a company's website may be inside a DMZ, granting FTP write access to computers in the intranet and HTTP read-only access to both networks.
The IP addresses within the DMZ can be public or private. In the latter case, pub-

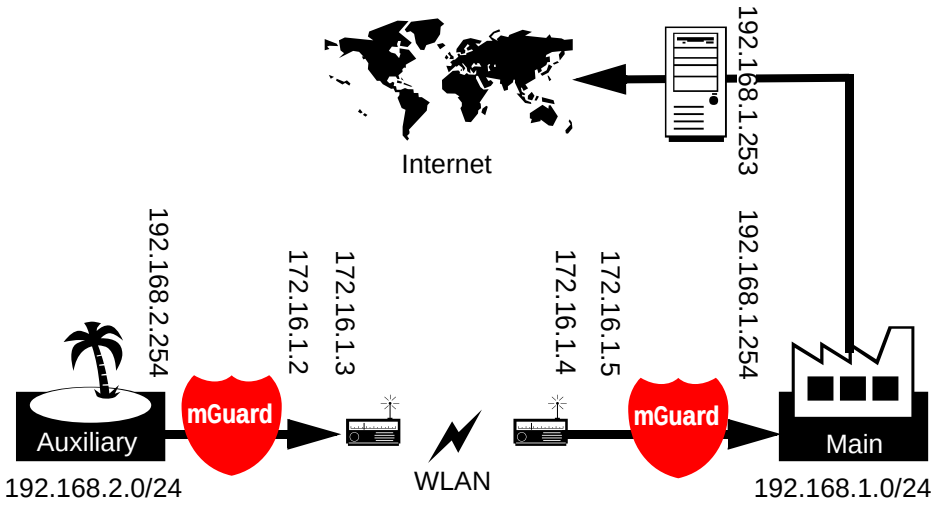
lic IPs would be mapped by means of portforwarding to the private addresses within the DMZ.

VPN Gateway



An encrypted access to the company's network is to be provided to employees at home or in the field. The mGuard thereby provides the services of a VPN gateway.
On the external computers an IPsec capable VPN client must be installed in case the computers operating system does not provide such a service, like Windows 2000 or XP do.

WLAN over VPN



Two buildings of a company are to be connected with an IPsec protected WLAN connection. From the auxiliary building it shall also be possible to use the main building's internet connection.

In this example the mGuards were switched into router mode and a separate network with addresses of 172.16.1.x was created for the WLAN. Since the internet should be also available via the VPN from the auxiliary building, a 'Default route over VPN' must be configured:

Connection type	Tunnel (Net <-> Net)
Local network address	192.168.2.0/24
Remote network address	0.0.0.0/0

In main building the appropriate counterpart to the connection is to be configured:

Connection type	Tunnel (Net <-> Net)
Local network address	0.0.0.0/0

Remote network address	192.168.2.0/24

The default route of an mGuard is usually directed to the external interface. But in this case the internet is reachable via 192.168.1.253 on the internal interface. Therefore, on the mGuard in the main building, an internal default route must be configured under “Network > Base”:

Additional Internal Routes	Network	Gateway
	0.0.0.0/0	192.168.1.253

and an external route to 172.168.1.2 and 172.168.1.3 must be added:

Additional External Routes	Network	Gateway
	172.16.1.2/1	172.16.1.4

3 Control and LEDs

LEDs	Colour	State	Meaning
2	Red/Green	red/green flashing	**Booting up**. After connecting the device to the power supply. After a few seconds, the LED will switch to a heartbeat.
	Green	flashing	**Heartbeat**. The device is correctly connected and functioning.
	Red	flashing	**System error**. ⌧ Perform a system restart. To accomplish this, briefly press the Recovery key (1.5 sec.) OR Disconnect the device from its power supply briefly and then reconnect it. If the error occurs again, start the *Recovery procedure* (see “Performing a Recovery” on page 91) or contact Support.
1 and **3**	Green	on or flashing	**Ethernet status**. LED 1 shows the status of the internal interface, LED 3 the status of the external interface. As soon as the device is connected to the interface (WAN or Internet), the LEDs will be on continuously to indicate that there is a connection to the network. The LEDs will flash when data packets are transferred.
1, 2, 3	various LED codes		**Recovery mode**. After pressing the **Recovery key** See “The Rescue Button – restart, recovery procedure and to flash the firmware” on page 91.

4 Startup

Safety instructions

The Innominate mGuard smart is intended for (protective) low voltage operation. Only connect the mGuard's network interfaces to LAN installations. Some telephone lines also use RJ45 jacks. The mGuard may not be operated on a telephone line.

Warning! This is a Class A device. It may cause radio interference in a living area, in which case, the operator may be requested to take appropriate measures.

General notes regarding usage

- Use a soft cloth to clean the case of the device. Do not use any aggressive solvents!
- Environmental conditions:
  0 to +40° Celsius,
  max. 90%, non-condensing humidity
- To avoid overheating, do not leave it in direct sunlight or expose it to any other source of heat.
- Do not bend the cables sharply. Only use network cables to connect to a network.

Steps for starting up the device

To startup the device, perform the following steps in the order listed:

Step	Objectives	Page
1	Check the package contents and read the Release Notes	"Package contents" on page 10
2	Connect the Device	"Connect the device" on page 11
3	Configure the device to the extent necessary. To accomplish this, select from the various options offered in the mGuard smart's configuration menus. For more information regarding which options and settings are required (or desirable) for your operating environment, please read the relevant sections in this manual.	"Local Configuration: At startup" on page 12

4.1 Package contents

Before beginning to setup the device, check that the package is complete:

Included in the package

- the mGuard smart
- a manual in the Portable Document Format (PDF) on the CD-ROM
- a Quick Installation Guide

4.2 Connect the device

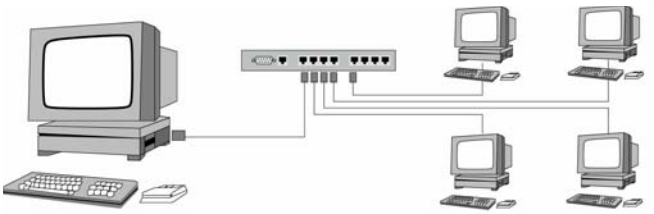
Ethernet plug to connect the unit directly to the system or network to be protected (**local** system or network).

USB connector to connect the unit to a computer's USB interface. Only used to supply power.

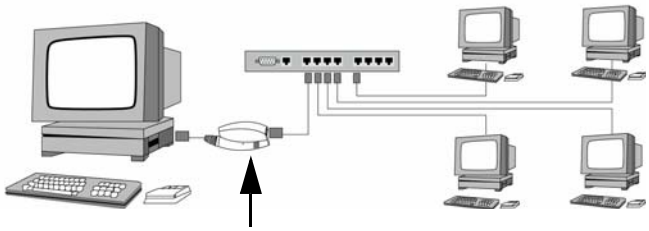
Jack for connecting an external network, e.g. WAN, Internet. (Connections to remote devices or networks are established via this network.)
Use a UTP cable (CAT 5).

If your system is already connected to a network, simply insert the mGuard between the system's network interface and the network.

before:



after:



- No additional driver needs to be installed.
- For reasons of security, we recommend that you change the default Root and Administrator passwords during the first configuration.

5 Configuration

Prerequisites

- The mGuard must be connected to a power-supply. In other words, its USB cable must be connected to a system (or power supply) that is ON.
- In a local configuration: The system that you use for performing the configuration must either be
  – connected to the mGuard's Ethernet connector,
  – or connected to it via the local network.
- In the case of a remote configuration: The mGuard smart must be configured to permit remote configuration.
- The mGuard must be connected, i.e. the required connections must function.

5.1 Local Configuration: At startup

The mGuard smart is configured using a Web browser, which is running on the configuration system (e.g. Firefox, MS Internet-Explorer or Safari)

⌧ The Web browser must support SSL (in other words https).

By default (factory settings), the mGuard smart is accessible at the following address:

Factory setting:

Stealth Mode (default setting): https://1.1.1.1/

With a configured network interface

In order for the mGuard to be accessed via the address https://1.1.1.1/, it must of course first be connected to a configured network interface. This is the case, if you insert it into an existing network connection - see the illustration in the section “Connect the device” on page 11.

In this case the Web browser can access the mGuard's configuration interface at the address https://1.1.1.1/ - see “Setting Up a Local Configuration Connection” on page 14. Continue from this point onwards in this case.

Without a configured network interface

If the computer’s network interface has not yet been configured

If the system, which will be used to configure the device, was not previously connected to a network, e.g. because the computer is new, its network interface will generally not be configured yet. This means that the system has not yet “been informed” that network traffic should be handled by this interface.

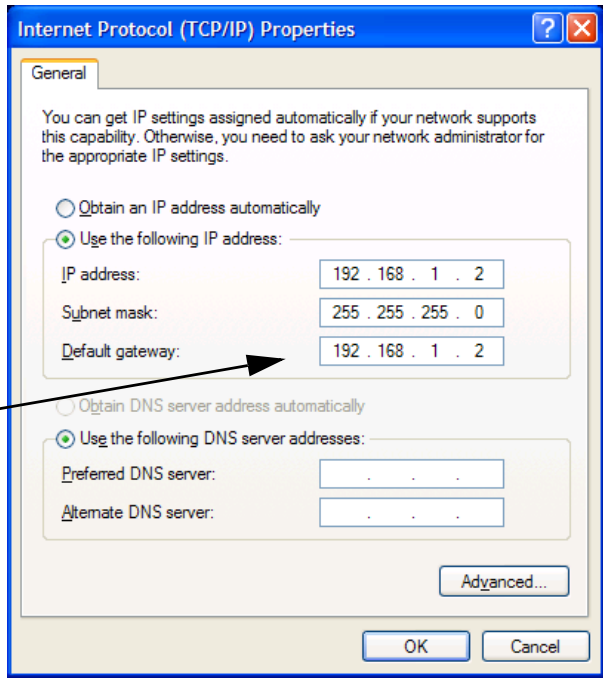
In this case, you must initialize the standard gateway by assigning it a dummy value. To accomplish this, proceed as follows:

Initializing the standard gateway

1. Determine the currently valid standard gateway address.
   If you are using Windows XP, click on **Start, Control Panel, Network Connections**: Right click on the icon of the LAN adapter and then click on **Properties** in the pop-up menu. In the dialog *Internet Protocol Properties* on the *General* tab, select **Internet Protocol (TCP/IP)** under “This connection

uses the following items” and then click on the **Properties** button to open the following dialog:

The IP address of the standard gateway can be examined or set here.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 2
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

If no IP address has been entered for the standard gateway in this dialog box, e.g. because *Obtain an IP address automatically* has been activated, enter the IP address manually. To do so, first activate **Use the following IP** and then enter, as an example, the following addresses:

IP address:	192.168.1.2
Subnetwork mask:	255.255.255.0
Standard gateway:	192.168.1.1

⌦ Do not under any circumstance assign the configuration system an address like 1.1.1.2!

2. On the DOS level (**Start, Programs, Accessories, Command Prompt**), enter:

   `arp -s` <IP of the standard gateway> **`aa-aa-aa-aa-aa-aa`**

   Example:

   You have determined that the address of the standard gateway is [or you have set it to]: 192.168.1.1

   Then the command should be:

   `arp -s 192.168.1.1 aa-aa-aa-aa-aa-aa`

3. To proceed with the configuration, first establish the necessary connection - see “Setting Up a Local Configuration Connection” on page 14.

4. After setting the configuration, restore the original setting for the standard gateway address. To do so, either restart the configuration computer or enter the following command at the DOS level [in the Command Prompt window]:

   `arp -d`

⌦ Depending on how you configure the mGuard, you may also need to modify the network interface settings of the locally connected system or network accordingly.

5.2 Setting Up a Local Configuration Connection

Web-based Administrator interface

The mGuard is configured using a Web browser, which is running on the configuration system (e.g. Firefox, MS Internet-Explorer or Safari)

⌦ **The Web browser must support SSL (in other words https).**

Depending on the mGuard's network mode (= mode of operation), it can be accessed (with the factory settings) at one of the following addresses:

Factory setting:

Stealth Mode (default setting):	https://1.1.1.1/
Router / PPPoE / PPPT Mode:	https://192.168.1.1/

Proceed as follows:

1. Start a Web browser.
   (For example, Firefox, MS Internet Explorer or Safari; the Web browser must support SSL (i.e. https).)
2. Make certain that the browser does not automatically dialup a connection when it is started because this could make it more difficult to establish a connection to the mGuard.
   In MS Internet Explorer, you can prevent this with the following setting: In the **Extras menu, select Internet Options...** and click on the *Connections*: tab.
   Make certain that *Never dial a connection* is selected under **Dial-up and Virtual Private Network settings**.
3. Enter the complete address of the mGuard into the browser's address field.
   In **Stealth** mode (= factory setting) this address always is

   `https://1.1.1.1/`

   and in **Router** , **PPPoE** or **PPTP** mode, the factory setting for the mGuard's address is

   `https://192.168.1.1/`

The mGuard's default IP address in *Stealth* mode: **https://1.1.1.1/** and not in *Stealth* mode: **https://192.168.1.1/**

Afterwards:
the mGuard's Administrator Web page will be displayed. The security notice shown under "After a connection has been successfully setup" on page 15 will displayed.

⌦ If you have forgotten the configured address:

If the address of the mGuard – in *Router*, *PPPoE* or *PPTP* mode – has been changed to a different value and you do not know the device's current address, you must use the **Recovery** key to restore it to Stealth mode and thus to the following address: https://1.1.1.1/ (see "Performing a Recovery" on page 91).

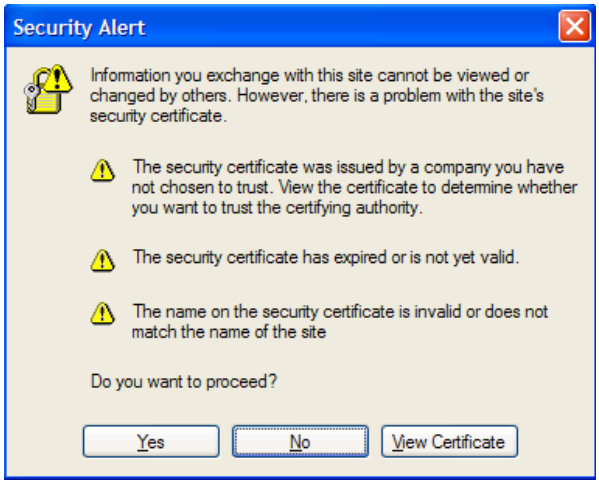
⌦If the Administrator Web page is not displayed...

If – even after repeated attempts – the Web browser still reports that the page cannot be displayed, try the following:

- Check whether the standard gateway has been initialized on the connected configuration system. See “Local Configuration: At startup” on page 12
- Try disabling any existing firewall.
- Make certain that the browser does not use a proxy server.
  In MS Internet Explorer (Version 6.0), you can prevent this with the following setting: In the **Extras menu, select Internet Options...** and click on the *Connections*: tab. Under *LAN Settings* click on the **Properties...** button and, in the *Local Area Network (LAN) Settings* dialog, check to make certain that **Use a proxy server for your LAN** (under Proxy server) is not activated.
- If any other LAN connection is active on the system, deactivate it until the configuration has been completed.
  Under the Windows **Start menu, Settings, Control Panel, Network Connections** or **Network and Dial-up Connections**, right click on the associated icon and select **Disable** in the pop-up menu.

After a connection has been successfully setup

After the connection has been successfully setup, the following security notice will be displayed (MS Internet Explorer):


Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate has expired or is not yet valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

Explanation:
Since administrative tasks can only be performed when a secure (encrypted) access has been established to the device, a signed (by the device) certificate will be returned.

Acknowledge the associated security notice by clicking on **Yes**.

Afterwards:
Once you have entered the correct user name (Login) and password, the Administrator Web page of the mGuard will be displayed.
The factory settings for these are:

Login: `admin`
Password: `mGuard`

⌦ These entries are case-sensitive!

To configure the device, proceed as follows:

Configuring the device

1. Select the page with the desired configuration options from the menu - see Page 18.
2. Make the desired settings on the associated page.

3. Once you have confirmed the changes by clicking on **OK**, the new settings will be activated on the device.
   The system will display a confirming message.

If the changes are not shown when you open the page again, because the browser has loaded the page from a cache, reload the page to refresh the display. To do so, click on the appropriate icon in the browser toolbar.

⌦ Depending on how you configure the mGuard, you may also need to modify the network interface settings of the locally connected system or network accordingly.

5.3 Remote Configuration

Prerequisite

The mGuard must be configured to permit remote configuration.

⌦ For reasons of security, remote configuration is disabled by default.

For information on how to enable remote configuration, see section “Access ‡ HTTPS” on page 72.

Performing a remote configuration

To configure the mGuard from a remote computer, first establish a connection between it and the local mGuard.
Proceed as follows:

1. Start a Web browser (e.g. Firefox, MS Internet Explorer or Safari; the Web browser must support SSL (i.e. https) on the remote system).
2. As the address, enter the IP address under which the remote site can be reached via the Internet or WAN, plus the port number.

   Example:
   If this mGuard can be found in the Internet at the address 123.456.789.21 and the Port Number 443 has been set as the port for remote access, you must enter the following address in the Web browser’s address field on the remote system: https://123.456.789.21/. If a different Port Number is used, this must be appended to the IP address, e. g.: https://123.456.789.21:442/

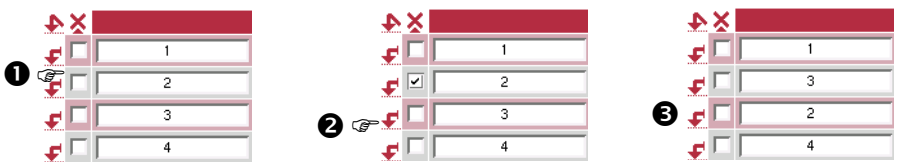
5.4 Working with tables

Insert row

1. Click on the arrow under which you want to insert a new row:

2. The new row is inserted.

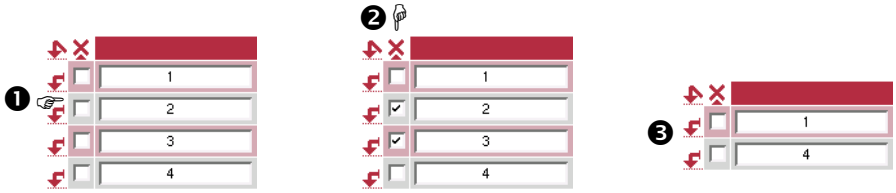
Move rows



1. Mark one or more rows you want to move.
2. Click on the arrow under which you want to move the marked rows:

3. The rows are moved.

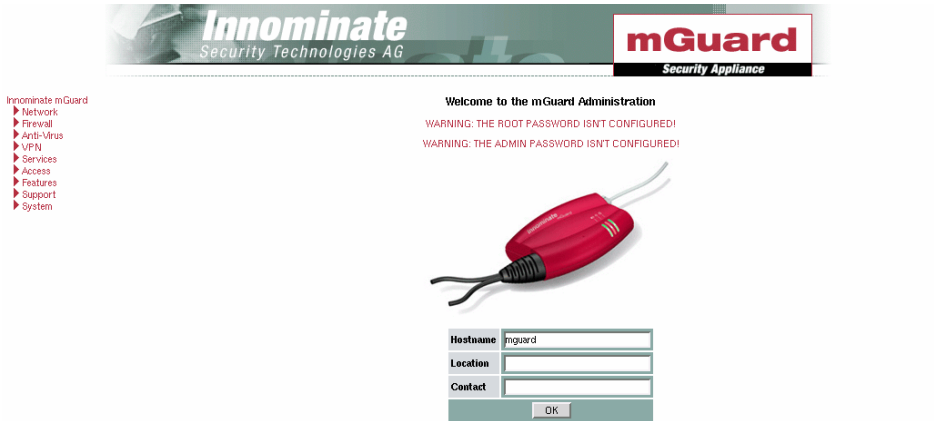
Delete rows



1. Mark the rows you want to delete.
2. Click on the symbol to delete the rows:

3. The rows are deleted.

5.5 Entry Page



On the entry page you can enter information which will help you and others to administer the mGuard:

Hostname

The hostname of this mGuard.

Contact

The name of the contact person for this mGuard, together with information on how to contact this person.

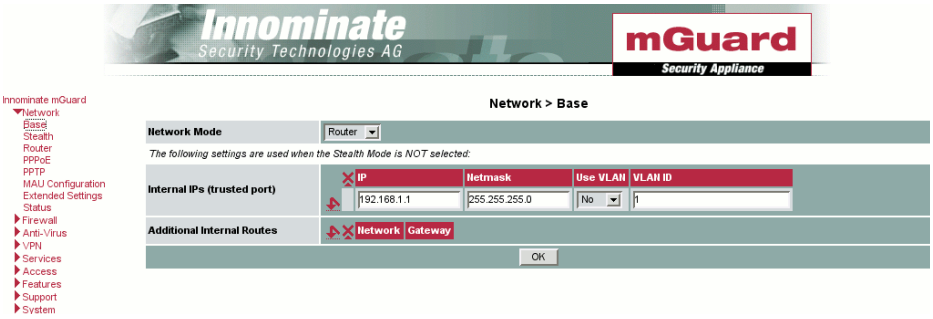
Location

The physical location of this mGuard.

⌦ For reasons of security, we recommend that you change the default Root and Administrator passwords during the first configuration - see “Access ‡ Passwords” on page 71. As long as the passwords have not been changed, you will see a notice on the entry page.

5.6 Network Menu

Network → Base



Network Mode

The mGuard must be set to the Network Mode (= operating mode) that matches its connection to the local computer or network. See “Typical application scenarios” on page 6.

See “Typical application scenarios” on page 6.

- When the Network Mode has been changed to or away from *Stealth* mode, the device will reboot automatically.
- If you change the address of the mGuard (e.g. by changing the Network Mode from *Stealth* to *Router*), the device will only be accessible at the new address. When the change is done from the local interface, you will get a message telling you the new address before the change becomes active. When the change is done from the external interface you will not receive feedback from the mGuard.
- If you set the Network Mode to *Router*, *PPPoE* or *PPTP* and then change the internal IP address and/or the local netmask, make very certain that you enter the correct values. Otherwise, the mGuard will no longer be accessible.

Transparent mGuard

Stealth (factory setting)

Stealth mode is only used when a single computer is locally connected to the device as a client.

In this mode, the device can be simply integrated (inserted) into an existing network connection of the respective computer. In this case, simply insert the mGuard into the network line - see the illustration in the section “Connect the device” on page 11.

The mGuard will analyze the network traffic passing through it and configure its network connection accordingly. It will then operate transparently, i.e. without requiring that the client be reconfigured.

As in the other cases, the mGuard supports the Firewall and VPN security functions in this mode of operation as well.

DHCP data (received from outside) will be passed through to the connected client.

- In case a firewall is installed on the client, it must be configured to allow ICMP Echo Requests (ping). Otherwise the mGuard won’t be able to use services like VPN, DNS, NTP, etc.
- The entries *Internal IPs* and *Additional internal routes* will be ignored. The IP 1.1.1.1 is used instead as the internal IP, which is accessible when the client’s configured default gateway is also accessible.

mGuard as router

The mGuard also operates as a router in PPPoE and PPTP mode.

Router

If the mGuard is not in *Stealth* mode, it serves as a gateway between different networks and has both an external and an internal IP address.

The external interface of the mGuard is connected via an Ethernet dedicated line to the Internet or via another router to a LAN.

A network or a single system is connected to its internal interface, the Ethernet plug. As in the other cases, the mGuard supports the Firewall and VPN security functions in this mode of operation as well.

- If the mGuard is operated in *Router* mode, you must set it as the standard gateway in the locally connected client computers. In other words, the address entered for the standard gateway must be the internal IP address of the mGuard. See “IP configuration on Windows clients” on page 66.
- If the mGuard is operated in *Router* mode and is used to establish the connection to the Internet, you should activate NAT to allow access to the Internet from the local network - see “Firewall ‡ NAT” on page 30. If NAT is not activated, the device will only allow VPN connections.

PPPoE

PPPoE mode corresponds to the Router mode with DHCP – with one difference: The PPPoE protocol, which is used by many DSL modems (for DSL Internet access), will be used, - as it is in Germany, for connecting to the external network (Internet or WAN). The external IP address, under which the mGuard can be reached from a remote site, is assigned by the Internet Service Provider.

- If the mGuard is operated in *PPPoE* mode, you must set it as the standard gateway in the locally connected client computers. In other words, the address entered for the standard gateway must be the internal IP address of the mGuard. See “IP configuration on Windows clients” on page 66.
- If the mGuard is in *PPPoE* mode, NAT must be activated to enable access to the Internet - see “Firewall ‡ NAT” on page 30. If NAT is not activated, the device will only allow VPN connections.

PPTP

This mode is similar to *PPPoE* mode. In Austria, for example, PPTP is used instead of the PPPoE protocol for DSL connections.
(PPTP is the protocol, which was originally used by Microsoft for VPN connections.)

- If the mGuard is operated in *PPTP* mode, you must set it as the standard gateway in the locally connected client computers. In other words, the address entered for the standard gateway must be the internal IP address of the mGuard. See “IP configuration on Windows clients” on page 66.
- If the mGuard is operated in *PPTP* mode, you should activate NAT to allow access to the Internet from the local network - see “Firewall ‡ NAT” on page 30. If NAT is not activated, the device will only allow VPN connections.

Internal IPs

The Internal IP is the IP address, under which the mGuard smart can be accessed from the locally connected LAN.

In **Stealth** mode, this address is always:

IP address:	**1.1.1.1**

In **Router** / **PPPoE** / **PPTP** mode, the default settings are:

IP address:	**192.168.1.1**
Local Netmask:	**255.255.255.0**

You can also specify other addresses, under which the mGuard can be accessed by devices on the locally connected network. This can be useful, for example, if the locally connected network is divided into subnetworks. In this

case, multiple units on different subnetworks can access the mGuard under different addresses.

IP

IP-Adresse, under which the mGuard shall be accessible on the internal interface (LAN).

Netmask

A netmask for the internal interface (LAN).

Use VLAN

If this IP address is to be inside a VLAN, this option must be set to **Yes**.

VLAN ID

A VLAN ID between 1 and 4095.

☞ An explanation of the term “VLAN” can be found under “VLAN” on page 100.

☞ Inserting, moving and deleting rows is explained under “Working with tables” on page 16.
(The first IP address in the list cannot be deleted.)

⌧ In *Stealth* mode, all additional internal IPs have no effect. In Stealth mode, the IP address is always: 1.1.1.1

Additional internal routes

In **Router** / **PPPoE** / **PPTP** mode:

If the locally connected network includes subnetworks, you can define additional routes.

Network

The network in CIDR notation – see “CIDR (Classless InterDomain Routing)” on page 89.

Gateway

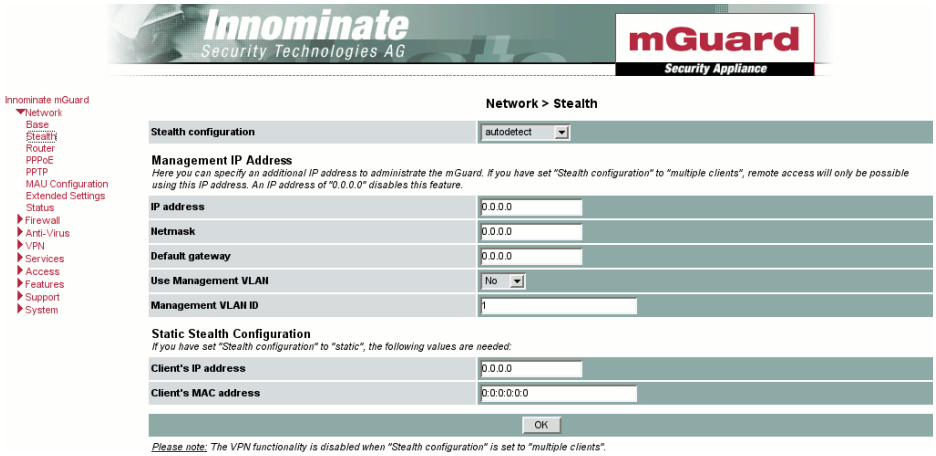
The gateway over which the network can be reached.

☞ An internal route to 0.0.0.0/0 defines a defaultroute over the internal interface. This one overrides any external defaultroutes.

☞ Inserting, moving and deleting rows is explained under “Working with tables” on page 16.

⌧ In *Stealth* mode, any additional internal routes have no effect.

Network → Stealth



Prerequisite: The mGuard must be set to the *Stealth* network mode.

Stealth configuration

autodetect

(Standard) The mGuard will analyse the network traffic and configure its network interface accordingly and will then function transparently.

For special cases, you can also preset these values, e.g. in the following case: The connected computer only accepts incoming connections so that it is not possible to configure the device automatically.

static

If the mGuard cannot analyse the network traffic passing through, e.g. because the locally connected computer only receives data, the *Stealth configuration* must be set to **Static**.

multiple clients

Like **autodetect**, but it is possible to use multiple devices and IPs on the mGuards internal interface (LAN).

For technical reasons VPN can't be used with this mode.

Management IP Address

An additional IP address can be specified here to administrate the mGuard. If

- *Stealth configuration* is set to the option **multiple clients** or
- the client doesn't answer ARP requests or
- there is no client at all,

then the remote administration via HTTPS, SNMP and SSH is only possible using the management IP address.

IP address

The additional IP address to contact the mGuard.

The IP address "0.0.0.0" disables the *Management IP Address*.

Netmask

The netmask for the IP address above.

Default Gateway

The default gateway of the network the mGuard is located in.

Use VLAN

If this IP address is to be inside a VLAN, this option must be set to **Yes**.

VLAN ID

A VLAN ID between 1 and 4095.

☞ An explanation of the term "VLAN" can be found under "VLAN" on page 100.

Static Stealth Configuration

IP-address of the clients

The IP-address of the client.

MAC-address of the client

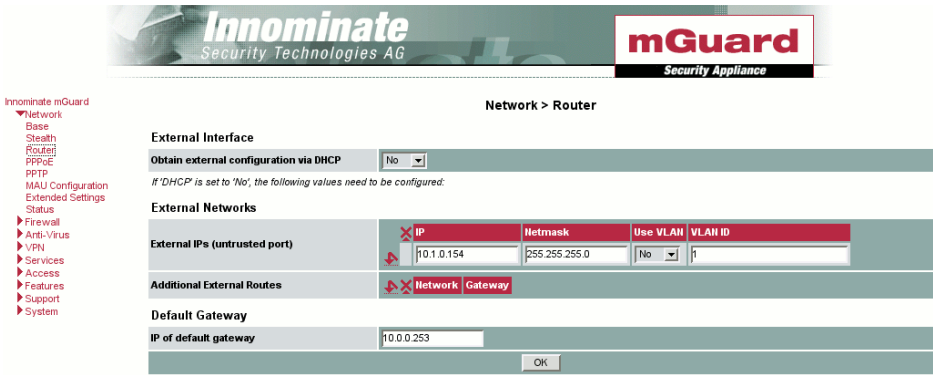
This is the physical address of the local computer's network adapter to which the mGuard is connected.

⌧ The MAC address can be determined in the following manner:

On the DOS level (**Start, Programs, Accessories, Command Prompt**), enter the following command:

```
ipconfig  /all
```

Network → Router



Prerequisite: The mGuard must be set to the *Router* network mode.

External Interface

Obtain external configuration via DHCP: Yes / No

☞ If the mGuard smart obtains the configuration data via DHCP (Dynamic Host Configuration Protocol) from a DHCP server, enter **Yes**. In that case, all other entries made on this page will be ignored.

☞ If the mGuard smart does not obtain the configuration data via DHCP (Dynamic Host Configuration Protocol) from a DHCP server, enter **No** and make the following additional entries:

External Networks

These are the addresses under which the mGuard can be accessed by devices in the external networks (connected to the mGuard's Ethernet connector). Form the interface to other parts of the LAN or Internet. If this unit is serving as a gateway to the Internet, the IP addresses will be assigned by the Internet Service Provider (ISP).

External IPs(untrusted port)

IP/Netmask

IP and netmask for the external interface (WAN).

Use VLAN

If this IP address is to be inside a VLAN, this option must be set to **Yes**.

VLAN ID

A VLAN ID between 1 and 4095.

☞ An explanation of the term "VLAN" can be found under "VLAN" on page 100.

☞ Inserting, moving and deleting rows is explained under "Working with tables" on page 16.
(The first address in the list can't be removed.)

Additional External Routes

In addition to the Default Route (see below), you can define additional, external routes.

☞ Inserting, moving and deleting rows is explained under “Working with tables” on page 16.

Default Gateway

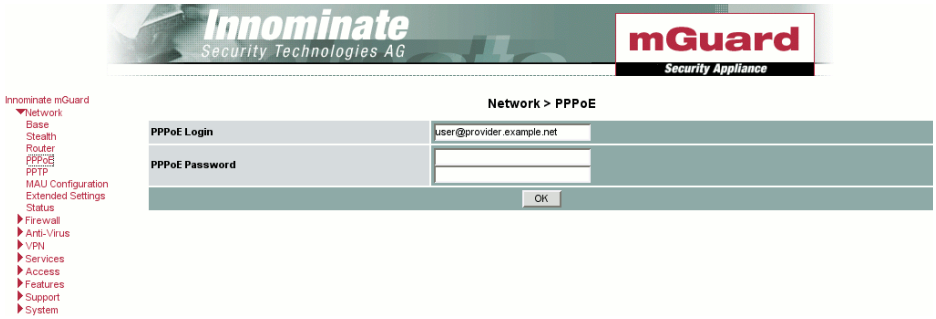
IP of default Gateway

This is defined by the Internet Service Provider (ISP), if the mGuard is used as a gateway to the Internet. If the mGuard is used within a LAN, this route is specified by the network administrator.

⌦ This setting will be ignored in case a local defaultroute is defined under “Network ‡ Base”.

⌦ If the local network is not known to the external router, e.g. in the case of configuration by DHCP, enter the address of your local network under Firewall → NAT, in other words 0.0.0.0/0 (see “Firewall ‡ NAT” on page 30)

Network → PPPoE



Prerequisite: The mGuard must be set to the *PPPoE* network mode. - see “PPPoE” on page 19.

In this field, enter the user name (Login) and password, which is expected by your Internet Service Provider (ISP) when you setup a connection to the Internet.

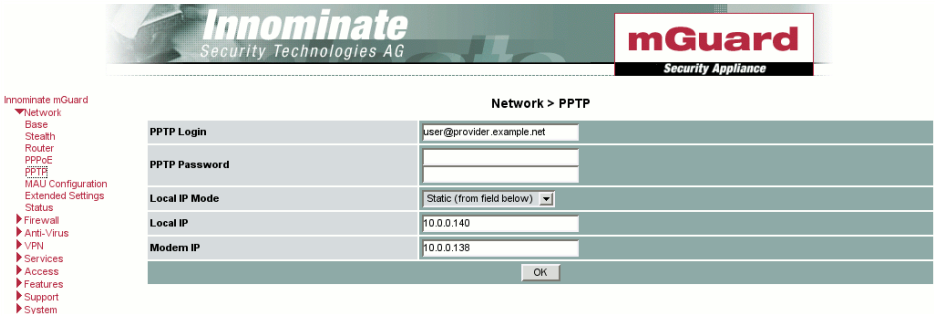
PPPoE Login

In this field, enter the user name (Login), which is expected by your Internet Service Provider (ISP) when you setup a connection to the Internet.

PPPoE Password

In this field, enter the password, which is expected by your Internet Service Provider when you setup a connection to the Internet.

Network → PPTP



Prerequisite: The mGuard must be set to the *PPTP* network mode. - see “PPTP” on page 19.

In this field, enter the user name (Login) and password, which is expected by your Internet Service Provider (ISP) when you setup a connection to the Internet.

PPTP Login

In this field, enter the user name (Login), which is expected by your Internet Service Provider when you setup a connection to the Internet.

PPTP Password

In this field, enter the password, which is expected by your Internet Service Provider when you setup a connection to the Internet.

Local IP Mode

Via DHCP

If the address data for the access to the PPTP server is supplied by the Internet Service Provider via DHCP, select **Via DHCP**.

In this case, you need not make an entry in the **Local IP** field.

Modem IP

This is the address of the Internet Service Provider's PPTP server.

Static (from field below)

If the address required to access the PPTP server is not supplied by the Internet Service Provider via DHCP, you must enter the IP address of the remote PPTP server and possibly that of the mGuard in the following two fields.

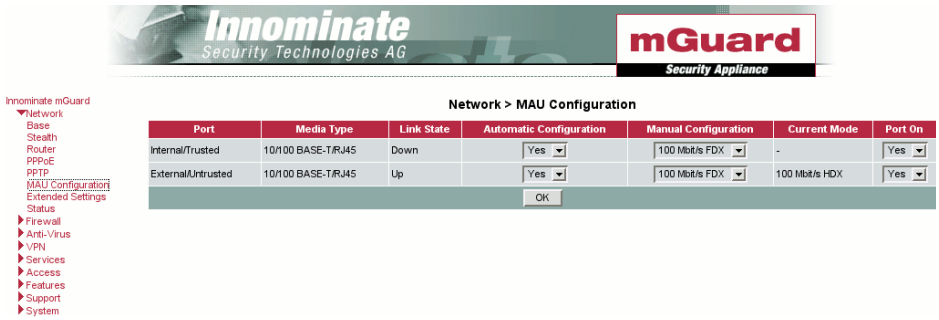
Local IP.

The IP address under which the mGuard can be accessed by the PPTP server.

Modem IP

This is the address of the Internet Service Provider's PPTP server.

Network → MAU Configuration (mGuard smart enterprise only)



Configuration and status display of the ethernet interfaces.

Port

Name of the interface the row refers to.

Media Type

Media type of the interface.

Link State

The state of the ethernet link which can be either **Up** or **Down**.

Automatic Configuration

When set to **Yes** the interface will be configured automatically. When set to **No**, the setting from the column **Manual Configuration** will be used.

⌧ Both ports of the mGuard smart are configured to be connected to a computer. If you connect the ports to a hub, please note that if *Automatic Configuration* is disabled, then the Auto-MDIX function will also be deactivated, i.e. the port of the mGuard has to be connected either to the uplink port of the hub or a cross-link cable has to be used.

Manual Configuration

The configuration for the interface to be used when **Automatic Configuration** is set to **No**.

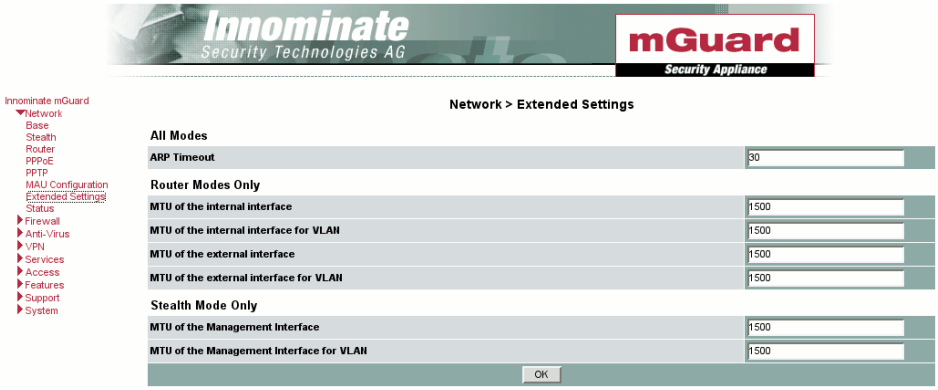
Current Mode

The current configuration of the interface.

Port on

Enables/disables the port.

Network → Extended Settings



All modes

ARP Timeout

Lifetime of entries in the ARP table.

Router Modes Only

MTU of the ... interface

The Maximum Transfer Unit (MTU) defines the maximal frame size when sending from this interface and is usually 1500 for ethernet interfaces.

Stealth Mode Only

MTU of the Management Interface

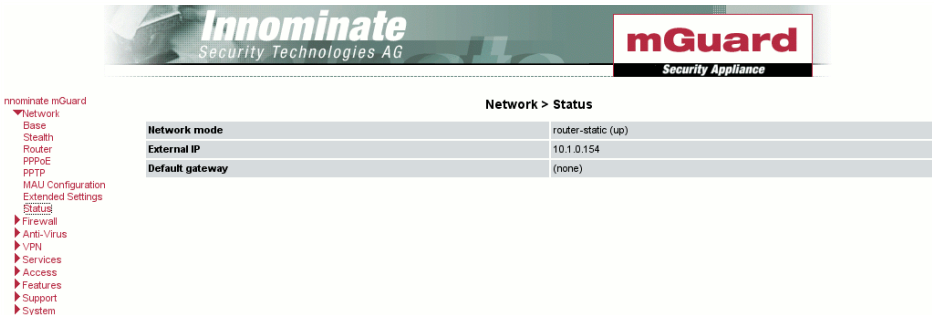
The Maximum Transfer Unit (MTU) defines the maximal frame size when sending from the management interface and is usually 1500 for ethernet interfaces.

MTU of the ... interface für VLAN

VLAN frames contain 4 bytes more than frames without VLAN which may cause problems with certain network equipment. By reducing the MTU from 1500 to 1496 such problems can be avoided.

Network → Status

Display only:



Network Mode

Displays the mGuard's current operating mode: *Stealth, Router, PPPoE* or *PPTP*. See “Network ‡ Base” on page 18.

External IP

This field shows the mGuard‘s IP address for the network interface used for its external network (WAN or Internet).
If the mGuard is assigned its IP address dynamically, you can view its currently valid IP address here.
In *Stealth* mode, the mGuard takes the address of the locally connected computer for this interface.

Default gateway:

The IP address over which the mGuard will route connections to networks unknown to him. In *Stealth* mode or in case the configured IP isn’t inside a known network this field will show “(none)”.

5.7 Firewall Menu

The mGuard has an integrated *Stateful Packet Inspection Firewall*. The connection data for each active connection is collected in a database (connection tracking). Therefore, it is only necessary to define rules for one direction – data from a connection‘s other direction – and only this will be automatically passed through. A side-effect is that (when reconfiguring) existing connections will not be dropped even if a corresponding new connection may not be setup.

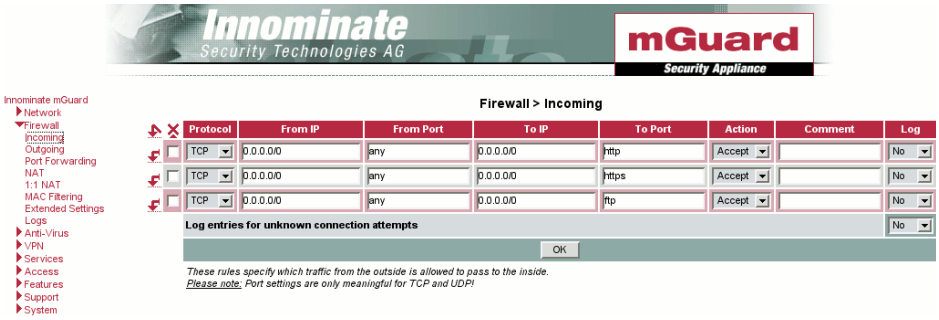
Factory settings for the firewall:

- All incoming connections will be rejected (except VPN).
- The data packets of all outgoing connections will be passed through.

⌦ VPN connections are not subject to the firewall rules defined in this menu. You can define firewall rules for each individual VPN connection in the **VPN → Connections** menu.

⌦ If multiple firewall rules are set, they will be searched in the order in which they are listed (from top to bottom) until a suitable rule is found. This rule will then be applied. If further down in the list there are other rules, which would also fit, they will be ignored.

Firewall → Incoming



Lists the firewall rules that have been set. These rules apply for incoming data connections, i.e. ones which were initiated by an external system.
If no rule has been set, all incoming connections (except VPN) will be dropped (= factory setting).

☞ Inserting, moving and deleting rows is explained under “Working with tables” on page 16.

⌦ There will be implicit rules for the protocols SMTP, HTTP and POP3 generated, that do not appear in the list of firewall rules, when activating the Anti-Virus function (see “Anti-Virus - Menu” on page 35).

You have the following options for the entries:

Protocol

All means: TCP, UDP, ICMP and other IP protocols.

IP address

0.0.0.0/0 means all addresses. To enter an address space, use the CIDR notation – see “CIDR (Classless InterDomain Routing)” on page 89.

Port

(This is only evaluated by the TCP and UDP protocols)

any means each and every port.

startport:endport (e.g. 110:120) defines a range of ports.

You can specify individual ports by giving either their port number or the corresponding service name: (e.g. 110 for pop3 or pop3 for 110).

Action

Accept means that the data packets are passed through.

Reject means that the data packets are rejected so that the sender is informed that the data packets have been rejected. (In *Stealth* mode, Reject has the same effect as Drop (see below).)

Drop means that the data packets are not passed through. The data packets will be discarded so that the sender will not be informed as to what happened to them.

⌧ In Stealth mode, **Reject** is not supported.

Comment

An informational comment for this rule.

Log

You can specify - for each individual firewall rule - whether the use of the rule

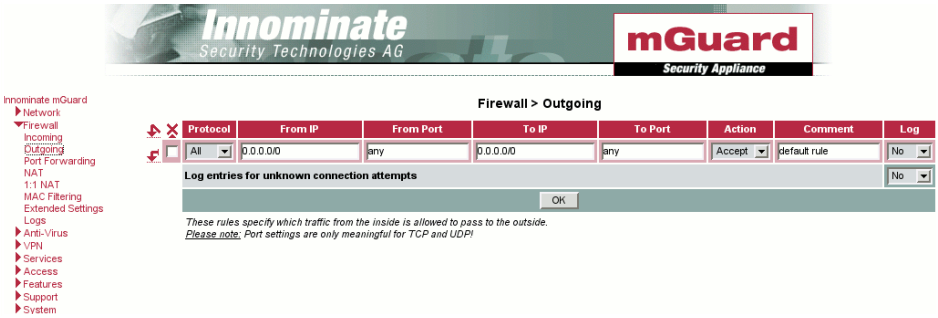
☞ should be logged by setting - *Log* to **Yes**

☞ or not by setting - *Log* to **No** (factory setting).

Log entries for unknown connection attempts

If this is set to Yes, all attempts to establish a connection, which were not covered by the rules defined above, will be logged.

Firewall → Outgoing



Lists the firewall rules that have been set. These rules apply for outgoing connections; i.e. ones which were initiated internally to communicate with a remote site.

The default (factory) setting is a rule that allows all outgoing connections.

If no rule is set, all outgoing connections are forbidden (except VPN).

☞ Inserting, moving and deleting rows is explained under “Working with tables” on page 16.

You have the following options for the entries:

Protocol

All means: TCP, UDP, ICMP and other IP protocols.

IP address

0.0.0.0/0 means all addresses. To enter an address space, use the CIDR notation – see “CIDR (Classless InterDomain Routing)” on page 89.

Port

(This is only evaluated by the TCP and UDP protocols)

any means each and every port.

startport:endport (e.g. 110:120) defines a range of ports.
You can specify individual ports by giving either their port number or the corresponding service name: (e.g. 110 for pop3 or pop3 for 110).

Action

Accept means that the data packets are passed through.

Reject means that the data packets are rejected so that the sender is informed that the data packets have been rejected. (In *Stealth* mode, Reject has the same effect as *Drop* (see below).)

Drop means that the data packets are not passed through. The data packets will be discarded so that the sender will not be informed as to what happened to them.

⌧ In Stealth mode, **Reject** is not supported.

Comment

An informational comment for this rule.

Log

You can specify - for each individual firewall rule - whether the use of the rule

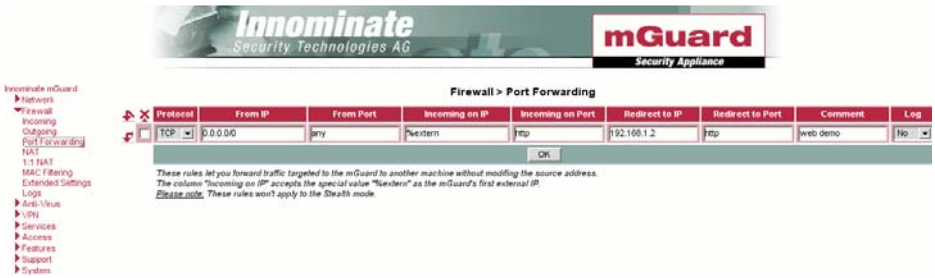
☞ should be logged by setting - *Log* to **Yes**

☞ or not by setting - *Log* to **No** (factory setting).

Log entries for unknown connection attempts

If this is set to Yes, all attempts to establish a connection, which were not covered by the rules defined above, will be logged.

Firewall → Port Forwarding



Lists the rules set for port forwarding.

Port forwarding performs the following: The headers of data packets incoming from the external network, which are addressed to the mGuard's external IP address (or one of its external IP addresses) and to one of the ports on the mGuard, will be rewritten to forward them to a specific port on a specific system in the internal network. In other words, both the IP address and the port number (in the header of the incoming data packets) will be changed.

This method is also called Destination NAT.

⌧ The rules set here have priority over the settings made in the **Firewall → Incoming** menu.

⌧ These rules don't apply to the stealth mode.

☞ Inserting, moving and deleting rows is explained under "Working with tables" on page 16.

Protocol

Specify the protocol which the rule should govern.

From IP

The source IP for which forwarding shall be performed.

From Port

The source port for which forwarding shall be performed.

Incoming on IP

Enter the external IP address (or one of the external IP addresses) of the mGuard here.

OR

If the destination IP address of the mGuard is assigned dynamically, this cannot be specified. In this case, use the following variable: **%extern**

⌦ The variable „%extern“ always corresponds to the first IP address of the address list, when using more than one static IP address.

Incoming on Port

The original destination port of the incoming data packets must be given in this field.

Redirect to IP

In this field, enter the internal IP address to which the data packets should be forwarded. The original destination address will be overwritten with the address entered in this field.

Redirect to Port

In this field, enter the port to which the data packets should be forwarded. The original entry for the destination port will be overwritten with the port specified in this field.

Comment

An informational comment for this rule.

You have the following options for the entries:

Port

You can specify individual ports by giving either their port number or the corresponding service name: (e.g. 110 for pop3 or pop3 for 110).

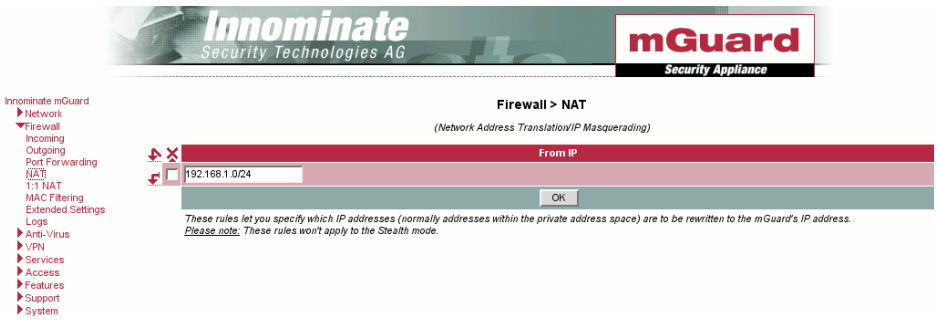
Log

You can specify - for each individual port forwarding rule - whether the use of the rule

☞ should be logged by setting - *Log* to **Yes**

☞ or not by setting - *Log* to **No** (factory setting).

Firewall → NAT



Lists the rules set for NAT (**N**etwork **A**ddress **T**ranslation).
In the case of outgoing data packets, the device can translate the sender‘s IP address (From IP) in the internal network to the device‘s own external address. This technique is called NAT (Network Address Translation).
This method is used whenever the internal address cannot or should not be routed externally, e.g. since it is in a private address space such as 192.168.x.x or because you wish to keep the internal network structure hidden.

This method is also called *IP-Masquerading*.

- If the mGuard is in *PPPoE/PPTP* mode, NAT must be activated to enable access to the Internet. If NAT is not activated, the device will only allow VPN connections.
- When using more than one IP address for an interface, always the first IP address of the list will be used for IP-Masquerading.
- These rules don't apply to the stealth mode.

Factory setting: NAT is not active.

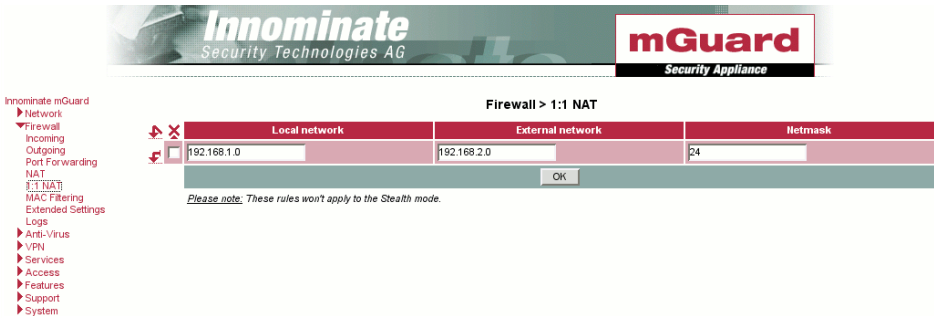
☞ Inserting, moving and deleting rows is explained under "Working with tables" on page 16.

You have the following options for the entries:

From IP

0.0.0.0/0 means all addresses, i.e. all internal IP addresses will be translated using NAT. To enter an address space, use the CIDR notation – see "CIDR (Classless InterDomain Routing)" on page 89.

Firewall → 1:1 NAT



Lists the rules set for 1:1 NAT (**N**etwork **A**ddress **T**ranslation), which mirrors addresses from the internal network into the external network.

In the following example the mGuard is inside the net 192.168.0.0/24 with its internal interface and inside the net 10.0.0.0/24 with its external interface. By using 1:1 NAT, the computer with the IP 192.168.0.8 can be reached under the IP 10.0.0.8 in the external network.

192.168.0.0/24 **10.0.0.0/24**

- These rules don't apply to the stealth mode.

Factory setting: NAT is not active.

☞ Inserting, moving and deleting rows is explained under "Working with tables" on page 16.

You have the following options for the entries:

Local network

The network address on the local interface (LAN).

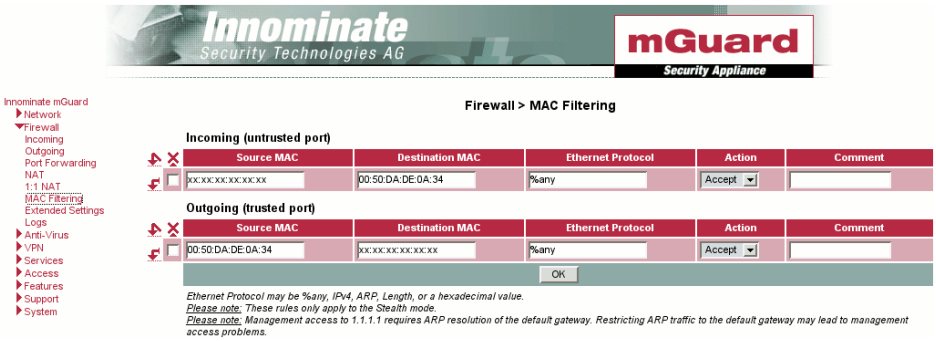
External network

The network address on the external interface (WAN).

Netmask

The network mask as a value between 1 and 32 for the local and extenal network address. (See also: “CIDR (Classless InterDomain Routing)” on page 89.)

Firewall → MAC Filtering



Beside the IP firewall (OSI Layer 3/4), which filters ICMP messages and TCP/UDP connections, the mGuard, when operating in stealth mode, can additionally filter for MAC addresses and ethernet protocols (OSI Layer 2).

In contrast to the IP firewall, the MAC filter is stateless. This means an additional rule must be created for some rules in the opposite direction where necessary.

When no rules are defined, all ARP and IP frames are allowed.

Incoming (untrusted port)

Outgoing (trusted port)

Source MAC

Definition of the source MAC address. **xx:xx:xx:xx:xx:xx** is a wildcard for all MAC addresses.

Destination MAC

Definition of the destination MAC address. **xx:xx:xx:xx:xx:xx** is a wildcard for all MAC addresses. The values **ff:ff:ff:ff:ff:ff** is the broadcast MAC address, to which, for example, all ARP requests are being sent.

Ethernet Protocol

%any is a wildcard for all ethernet protocols. Protocols can be specified by name or hexadecimal value, for example:

- IPv4 or 0800
- ARP or 0806

Action

Accept means that frames can pass.

Drop means to drop frames.

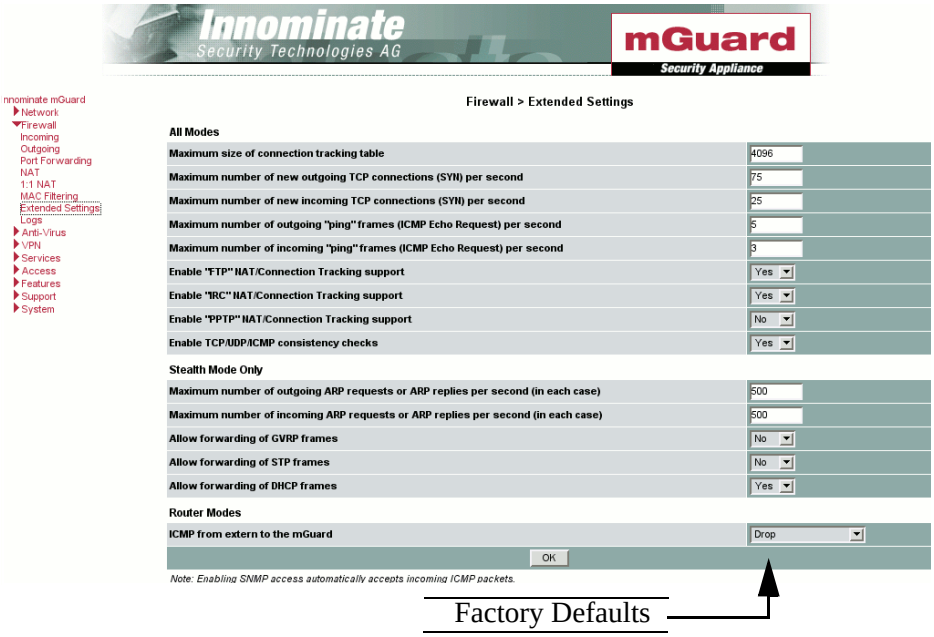
Comment

An informational comment for this rule.

☒ The MAC filter does not support logging.

☒ Rules defined here supercede the IP firewall rules.

Firewall → Extended Settings



The settings affect the fundamental behaviour of the firewall. The factory defaults can be seen in the figure above.

All modes

Maximum number of ...

These 5 settings define upper limits. They are so selected that they are never reached in normal operation. However, since they can be easily reached in the event of an attack, the limits provide additional security. If your operational environment has special requirements, you can increase these values.

Enable “FTP” NAT/Connection Tracking support

If an outgoing FTP (protocol) connection is setup to download data, there are two alternatives as to how the data will be transmitted: When using “active FTP” the server called will call the calling system back to establish a connection for the transfer of data. When using “passive FTP” the calling system will establish this additional connection for the data transfer. To let the data of this additional connection pass through the firewall, **Enable “FTP” NAT/Connection Tracking support** must be set to **Yes** (factory setting).

Enable "IRC" NAT/Connection Tracking support

This is similar to “FTP”: When the IRC protocol is used for chatting in the Internet, incoming connections must also be permitted after the connection has been established actively. In this case, **Enable “IRC” NAT/Connection Tracking support** must be set to **Yes** so that the firewall will permit these connections (factory setting).

Enable "PPTP" NAT/Connection Tracking support

This need only be set to **Yes** under the following condition:
if a local system should establish a VPN connection via PPTP to an external system without help from the mGuard.
The factory setting is **No**.

Enable TCP/UDP/ICMP consistency checks

When set to **Yes** the mGuard performs various checks for wrong check sums, packet sizes, etc. and drops packets failing the check.

Stealth Mode Only

Maximum number of outgoing ARP requests or ARP replies per second (in each case)

Maximum number of incoming ARP requests or ARP replies per second (in each case)

These two settings define maximum values for the allowed maximum number of incoming and outgoing ARP-request per second. They are so selected that they are never reached in normal operation. However, since they can be easily reached in the event of an attack, the limits provide additional security. If your operational environment has special requirements, you can increase these values.

Allow forwarding of GVRP frames

The GARP VLAN Registration Protocol (GVRP) is used by GVRP capable switches to exchange configuration information.

By setting this switch to **Yes**, GVRP frames are allowed to traverse the mGuard in Stealth Modus.

Allow forwarding of STP frames

The Spawning-Tree Protocol (STP) (802.1d) is used by bridges and switches to detect and avoid loops in the network topology.

By setting this switch to **Yes**, STP frames are allowed to traverse the mGuard in Stealth Modus.

Allow forwarding of DHCP frames

Allow the client to retrieve an IP address using DHCP independently from the outgoing firewall rules as these won't become active until the mGuard has learned the clients IP.

This switch is set to **Yes** per default.

ICMP from extern to the mGuard

With this option you can control which ICMP messages from the external network are accepted by the mGuard. You have the following options:

Drop: All ICMP-messages sent to the mGuard from the external network will be dropped.

Allow ping requests: Only ping requests (ICMP message type 8) from the external network will be accepted.

Allow all ICMPs: All ICMP messages from the external network will be accepted.

Firewall → Logs

If the logging of events was activated (Log = Yes) on the firewall rules page, you can view the log with all of the recorded events here.

The format of the log corresponds to that common under Linux.

Display only:

Special analysis programs are available which can be used to present the information from the log in a more readable format.

5.8 Anti-Virus - Menu

The Innominate mGuard's anti-virus function offers protection against infiltration by viruses sent via the HTTP, POP3 and SMTP protocols.

Kaspersky Engine

The data blocks transferred in an e-mail or during an HTTP connection are filtered out, if necessary decompressed, and then checked with the Kaspersky virus filter.

To accomplish this a port-redirection rule is added to the firewall, which internally redirects the connection to a transparent proxy.

In the event that a virus is detected, the system will - depending on the protocol - send an e-mail with an error message to the user, generate an error message and add an entry to the anti-virus log. If the virus filter does not find a virus, the data block will be forwarded unchanged by the proxy.

In the following sections, you will find details for each respective protocol.

Supported compression formats

The virus filter can decompress the following formats:

- ZIP
- RAR
- Mail
- Embedded (RFC822 MIME attachment to an e-mail, MS OLE, including gzipped embedded scripts).
- GZIP
- Compress

Work is currently in progress to provide support for other formats (Trap and UPX).

Prerequisites for use

The following prerequisites must be satisfied to use the virus filter:

- The Anti-Virus license must be installed. The “Anti-Virus” menu is only activated when the license is installed. For instructions on how to request and install a license, please read the section **Anti-Virus -> License Request**.
- An Update Server with the current versions of the virus signatures (see **Anti-Virus -> Database Update**).
- Configuration and activation of the Anti-Virus protection (see the following sections for the respective protocol)

Anti-Virus License expiration

If your anti-virus license is expired, the further database update will be locked. “Anti-Virus Update Status” will show the message “locked ([45] kavupdater licence expired)”. After you installed a valid anti-virus license, please use the button **Unlock Database Update** in the “Anti-Virus Update Status” menu to unlock the database update.

After expiration of your anti-virus license, the Innominate AG reserves itself the right to delete the virus signatures in case the storage capacity is exceeded during a software update (See “Update running” on page 48.).

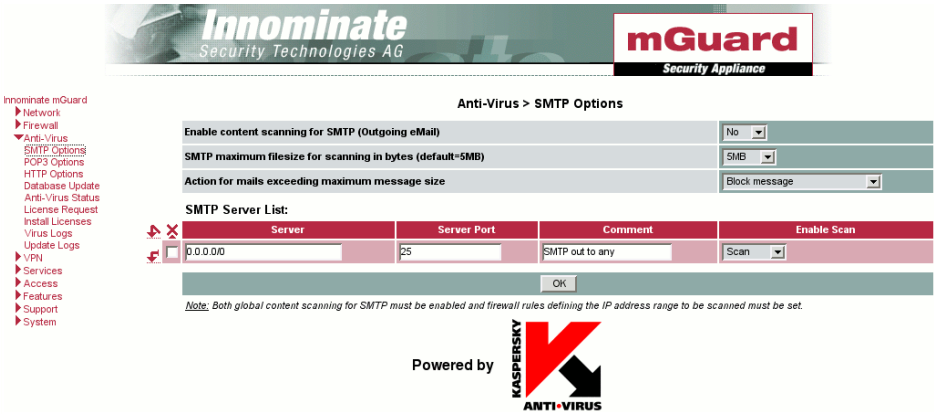
File size - limiting

Due to the mGuard's limited memory there are - compared to conventional virus filters - a few differences which must be considered.

Each of the files to be checked must first be copied in its entirety to the mGuard's RAM disk so that the virus filter can decompress it and check it for viruses. Since the Innominate mGuard monitors multiple connections at the same time to support e.g. parallel e-mail clients and web browsers, the limited amount of memory available may form a bottleneck. To avoid this bottleneck, set the maximum size of the files to be checked in the menu. The default value set for the maximum size will ensure trouble free operation of the anti-virus filter in most cases so please do not change this setting unless you need to.

In the menu, you can choose whether - in the event that the maximum size is exceeded - the system should block the data and send an error message to you or let the data pass unscanned.

Anti-Virus → SMTP Options



The SMTP protocol is used by e-mail clients or mail transfer agents (MTA) to send e-mails.

☞ The virus filter can only check unencrypted data for viruses.

Consequently, you should not activate encryption options such as TLS. If a virus is detected or an error occurs, an e-mail with an error code will be sent to the sender and an entry will be made in the anti-virus log. The intended recipient will receive neither the infected mail nor a message.

Enable content scanning for SMTP (outgoing e-mail)

Use this option to activate (set to “Yes”) or deactivate (set to “No”) the virus filter. When this option is activated, the system will set up a port redirection for SMTP connections, which redirects them to the SMTP proxy.

SMTP maximum filesize for scanning in bytes (default=*x* MB)

With this parameter, you can set the maximum size of the files to be checked.

If this limit is exceeded, the system will - depending on the setting “Action for mails exceeding maximum message size” - block the e-mail and send an error message back to the e-mail client or it will automatically switch to the “Let the message pass unscanned” mode.

If the mGuard does not have enough memory to save a file completely or to decompress it, a corresponding error message will be sent to the user's e-mail client and an entry will be written to the anti-virus log. In this case, you have the following options:

- You can try again later to send the message.
- You can temporarily deactivate the virus filter for the corresponding server
- You can set the parameter to “Let the message pass unscanned”.

Please note that - depending on the coding scheme used - the size of the attachment may be larger than the original file.

Action for mails exceeding the maximum message size

Let the message pass unscanned

When this option is selected the virus filter will allow the messages, which exceed the filesize set, to pass through unscanned.

☞ In this case, the message is not checked for viruses!

Block message

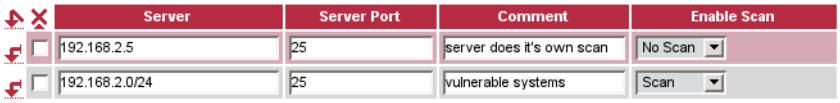
When this option is selected, an error code will be returned to the e-mail client and the e-mail will be blocked.

SMTP Server List

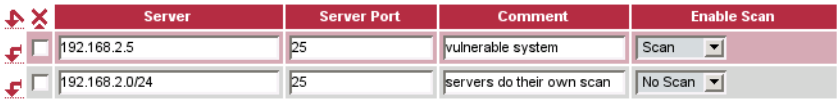
You can enter a list of the servers, whose traffic should be filtered, and specify for each IP address whether or not the anti-virus protection should be activated. It is also possible to enter “trusted” servers.

Examples:
Global activation of the anti-virus protection for SMTP:

Scan a subnet and exclude a SMTP server:



Scan traffic to a single SMTP server in a subnet:



☞ Inserting, moving and deleting rows is explained under “Working with tables” on page 16.

- The set of rules will be processed from the top down, therefore, the order of the rules is also decisive for the results.
- The virus filter can only handle a limited number of simultaneous connections to mail, HTTP and FTP servers. Exceeding this number will cause further connection attempts to be refused.
- If the SMTP virus filter is activated, the firewall will open the corresponding ports regardless of whether there are any firewall rules to the contrary.

You have the following options for the entries:

Server

0.0.0.0/0 means all addresses, i.e. the system will filter the traffic to all SMTP servers. To enter an address space, use the CIDR notation – see “CIDR (Classless InterDomain Routing)” on page 89.

- Since an attempt to setup a connection is first handled by the proxy, if a nonexistent server is requested (e.g. a bad IP address) the user software will act as though the connection to the server had been established, but no data was sent. If the list contains the exact server addresses, this behavior can be prevented, since the proxy will then only take requests addressed to the servers given in the list.

Server Port

Enter the number of the port for the SMTP protocol in this field. The default setting for the SMTP port is **25**.

Comment

An informational comment for this rule.

Scan

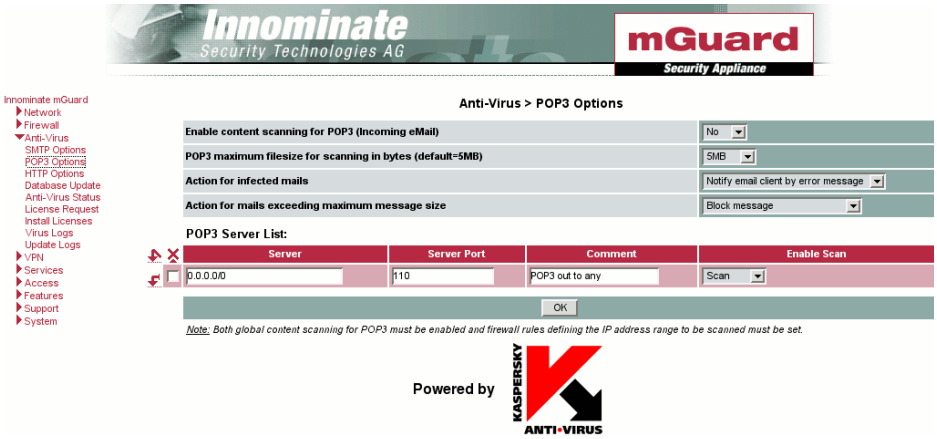
Scan

The virus filter is activated for the server specified in this rule.

No Scan

The virus filter is deactivated for the server specified in this rule.

Anti-Virus → POP3 Options



Your e-mail client uses the POP3 protocol for incoming e-mail.

☞ The virus filter can only check unencrypted data for viruses. Consequently, you should not activate encryption options such as STLS or SSL. Encrypted authentication using AUTH is, however, usable, since the e-mail itself is not encrypted.

Enable content scanning for POP3 (incoming e-mail)

Use this option to activate (set to “Yes”) or deactivate (set to “No”) the virus filter. When this option is activated, the system will set up a port redirection for POP3 connections, which redirects them to the POP3 proxy.

☞ Tip: When using a POP3 connection, most e-mail clients will pick up all of the e-mails during a single connection. In this case, the new settings will first take effect after the last e-mail is collected from the server during the current connection. Consequently, to change the settings when an e-mail transfer is in process, first cancel the transfer.

POP3 maximum filesize for scanning in bytes (default=*x* MB)

With this parameter, you can set the maximum size of the files to be checked. If this limit is exceeded, the system will - depending on the setting “Action for mails exceeding the maximum message size” - block the e-mail and send an error message back to the e-mail client or it will automatically switch to “Let the message pass unscanned” mode.

If the mGuard does not have enough memory to save a file completely or to decompress it, a corresponding error message will be sent to the user's e-mail client and an entry will be written to the anti-virus log. In this case, you have the following options:

- You can try again later to download the file
- You can temporarily deactivate the virus filter for the corresponding server
- You can set the parameter to “Let the message pass unscanned”.

Please note that - depending on the coding scheme used - the size of the attachment may be larger than the original file.

Action for infected mails

Notify recipient by e-mail:

If the virus filter detects a virus, the recipient will be informed by e-mail.

Notify e-mail client by error message:
If the virus filter detects a virus, the recipient will be informed by an error message sent to the e-mail client.

☞ If the parameter “Delete received messages from server” has been set in the e-mail client software and the “Action for infected mails” has been set to “Notify recipient by e-mail”, the infected e-mail will be deleted on the server, since the e-mail client will assume that the e-mail has been successfully transferred. If you do not wish to have the infected mail deleted (e.g. if you wish to download the infected e-mail in some other manner), only use the option “Notify e-mail client by error message”.

Action for mails exceeding the maximum message size

Let the message pass unscanned
When this option is selected the virus filter will allow the messages, which exceed the filesize set, to pass through unscanned.

☞ In this case, the mail will not be checked for viruses!

Block message
When this option is selected, an error code will be returned to the e-mail client and the e-mail will be blocked.

POP3 Server List

You can select the servers, whose traffic should be filtered, and specify for each IP address whether or not the anti-virus protection should be activated. It is also possible to enter “trusted” servers.

Examples:
Global activation of the anti-virus protection for POP3:

Server	Server Port	Comment	Enable Scan
0.0.0.0/0	110	POP3 out to any	Scan

Scan a subnet and exclude a “trusted” POP3 server:

Server	Server Port	Comment	Enable Scan
192.168.2.5	110	trusted POP3	No Scan
192.168.2.0/24	110	untrusted POP3	Scan

Scan a single “untrusted” POP3 server in a subnet:

Server	Server Port	Comment	Enable Scan
192.168.2.5	110	untrusted POP3	Scan
192.168.2.0/24	110	trusted POP3	No Scan

☞ Inserting, moving and deleting rows is explained under “Working with tables” on page 16.

⌧ To activate use the anti-virus protection for HTTP or “FTP over HTTP” through a proxy, add a new line to the HTTP server list and change the predefined port 80 to the proxy port of your webbrowser.
Port numbers used commonly are 3128 or 8080.

⌧ The set of rules will be processed from the top down, therefore, the order of the rules is also decisive for the results.

⌧ The virus filter can only handle a limited number of simultaneous connections

to mail, HTTP and FTP servers. Exceeding this number will cause further connection attempts to be refused.

⌦ If the POP3 virus filter is activated, the firewall will open the corresponding ports regardless of whether there are any firewall rules to the contrary.

You have the following options for the entries:

Server

0.0.0.0/0 means all addresses, i.e. the system will filter the traffic of all POP3 servers. To enter an address space, use the CIDR notation – see “CIDR (Classless InterDomain Routing)” on page 89.

⌦ Since an attempt to setup a connection is first handled by the proxy, if a nonexistent server is requested (e.g. a bad IP address) the user software will act as though the connection to the server had been established, but no data was sent. If the list contains the exact server addresses, this behavior can be prevented, since the proxy will then only take requests addressed to the servers given in the list.

Server Port

Enter the number of the port for the POP3 protocol in this field. The default setting for the POP3 port is **110**.

Comment

An informational comment for this rule.

Scan

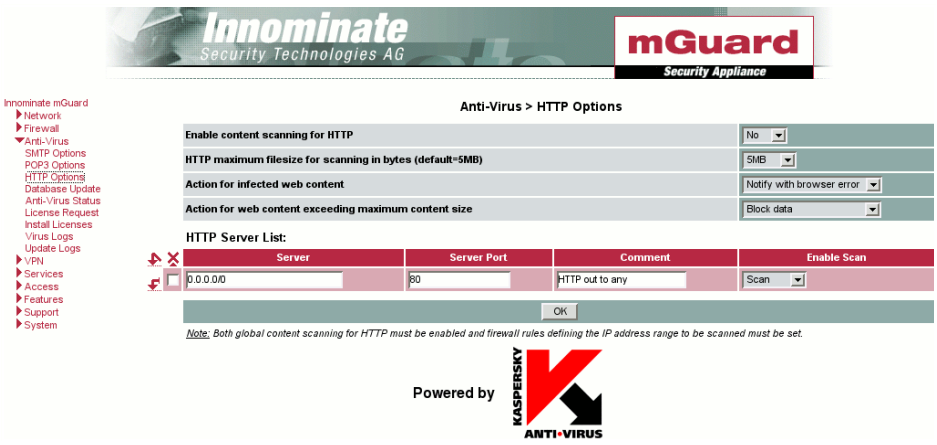
Scan

The virus filter is activated for the servers specified in this rule.

No Scan

The virus filter is deactivated for the server specified in this rule.

Anti-Virus → HTTP Options



The HTTP protocol is not only used by web browsers to retrieve data from web sites, but is also used in many other applications. It is also used, for example, to download files, e.g. software updates, or to initialize multimedia streams.

The transferred file will only passed on after it has been loaded completely and checked. Consequently, user software may react less quickly when downloading larger files or whenever the download speeds are slow.

⌦ To check the anti-virus protection for HTTP, you can download the safe Eicar test virus which is available for test purposes at http://www.eicar.org/anti_virus_test_file.htm.

Enable content scanning for HTTP

Use this option to activate (set to “Yes”) or deactivate (set to “No”) the virus filter. When this option is activated, the system will set up a port redirection for HTTP connections, which redirects them to the HTTP proxy.

HTTP maximum filesize for scanning in bytes (default=*x* MB)

With this parameter, you can set the maximum size of the files to be checked.

If this limit is exceeded, the system will send an error message to the browser or automatically switch to “Let the data pass unscanned” mode.

If the mGuard does not have enough memory to save a file completely or to decompress it, a corresponding error message will be sent to the user's client software (browser or download manager) and an entry will be written to the anti-virus log. In this case, you have the following options:

- You can try again later to download the file
- You can temporarily deactivate the virus filter for the corresponding server
- You can set the parameter to “Let the data pass unscanned”.

Action for infected web content

Notify with browser error

If the virus filter detects a virus in the data transferred from an HTTP server to the HTTP client, an error message will be sent to the HTTP client. The handling of this error message depends on the respective HTTP client. A web browser will display the error message in the form of an HTML page. If a file that is downloaded within an HTML page - e.g. a graphic file - is infected, this file will not be displayed in the browser. If a download manager is used to download a file via HTTP, the error message will be displayed by the download manager.

Action for web content exceeding the maximum content size

Let data pass unscanned

When this option is selected the virus filter will allow the files, which exceed the filesize set, to pass through unscanned.

☞ In this case, the data is not checked for viruses!

Block data

If this option is selected, the system will terminate the download and send an error message to the client software whenever the content exceeds the maximum size.

HTTP Server List

You can select the servers, whose traffic should be filtered, and specify for each IP address whether or not the anti-virus protection should be activated. It is also possible to enter “trusted” servers.

Examples:

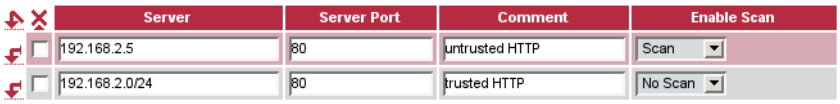
Global activation of the anti-virus protection for HTTP:

	Server	Server Port	Comment	Enable Scan
	0.0.0.0/0	80	HTTP out to any	Scan

Scan a subnet and exclude a “trusted” HTTP server:

	Server	Server Port	Comment	Enable Scan
	192.168.2.5	80	trusted HTTP	No Scan
	192.168.2.0/24	80	untrusted HTTP	Scan

Scan a single “untrusted” HTTP server in a subnet:



☞ Inserting, moving and deleting rows is explained under “Working with tables” on page 16.

- To activate the virus filter for HTTP or “FTP over HTTP” connections over a proxy, insert a new row and change the default port 80 to the proxy’s port. Common proxy ports are 3128 and 8080.
- The set of rules will be processed from the top down, therefore, the order of the rules is also decisive for the results.
- The virus filter can only handle a limited number of simultaneous connections to mail, HTTP and FTP servers. Exceeding this number will cause further connection attempts to be refused.
- If the HTTP virus filter is activated, the firewall will open the corresponding ports regardless of whether there are any firewall rules to the contrary.

You have the following options for the entries:

Server

0.0.0.0/0 means all addresses, i.e. the system will filter the traffic of all HTTP servers. To enter an address space, use the CIDR notation – see “CIDR (Classless InterDomain Routing)” on page 89.

- Since an attempt to setup a connection is first handled by the proxy, if a nonexistent server is requested (e.g. a bad IP address) the user software will act as though the connection to the server had been established, but no data was sent. If the list contains the exact server addresses, this behavior can be prevented, since the proxy will then only take requests addressed to the servers given in the list.

Server Port

Enter the number of the port for the HTTP protocol in this field. The default setting for the HTTP port is **80**.

Comment

An informational comment for this rule.

Scan

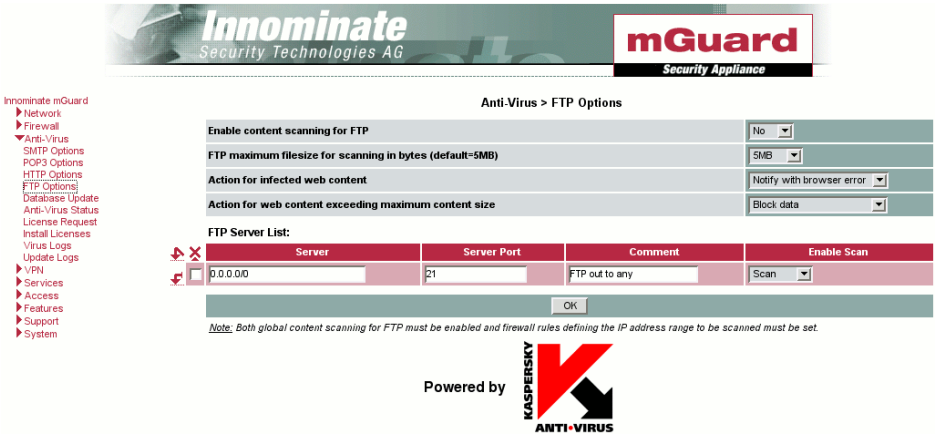
Scan

The virus filter is activated for the server specified in this rule.

No Scan

The virus filter is deactivated for the server specified in this rule.

Anti-Virus → FTP Options



The FTP protocol is used for up- and download of files.

☞ The transferred file will only passed on after it has been loaded completely and checked. Consequently, user software may react less quickly when downloading larger files or whenever the download speeds are slow.

☞ To check the anti-virus protection for FTP, you can download the safe Eicar test virus which is available for test purposes at ftp://ftp.kaspersky.com/utils/eicar/EICAR.COM.

Enable content scanning for FTP

Use this option to activate (set to “Yes”) or deactivate (set to “No”) the virus filter. When this option is activated, the system will set up a port redirection for FTP connections, which redirects them to the FTP proxy.

FTP maximum filesize for scanning in bytes (default=*x* MB)

With this parameter, you can set the maximum size of the files to be checked.

If this limit is exceeded, the system will send an error message to the browser or automatically switch to “Let the data pass unscanned” mode.

If the mGuard does not have enough memory to save a file completely or to decompress it, a corresponding error message will be sent to the user's client software and an entry will be written to the anti-virus log. In this case, you have the following options:

- You can try again later to download the file
- You can temporarily deactivate the virus filter for the corresponding server
- You can set the parameter to “Let the data pass unscanned”.

Action for infected web content

Notify with browser error

If the virus filter detects a virus in the data transferred from an FTP server to the FTP client, an error message will be sent to the FTP client. The handling of this error message depends on the respective FTP client.

Action for web content exceeding the maximum content size

Let data pass unscanned

When this option is selected the virus filter will allow the files, which exceed the filesize set, to pass through unscanned.

⌧ In this case, the data is not checked for viruses!

Block data

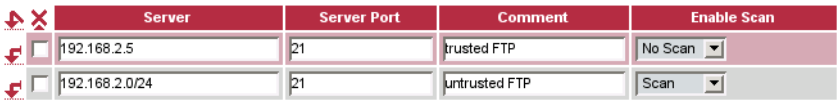
If this option is selected, the system will terminate the download and send an error message to the client software whenever the content exceeds the maximum size.

FTP Server List

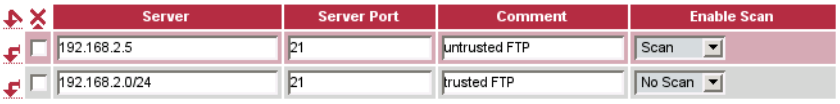
You can select the servers, whose traffic should be filtered, and specify for each IP address whether or not the anti-virus protection should be activated. It is also possible to enter “trusted” servers.
Examples:

Global activation of the anti-virus protection for FTP:

Scan a subnet and exclude a “trusted” FTP server:



Scan a single “untrusted” FTP server in a subnet:



☞ Inserting, moving and deleting rows is explained under “Working with tables” on page 16.

- To activate the virus filter for FTP connections over a proxy, insert a new row and change the default port 21 to the proxy’s port.
- The set of rules will be processed from the top down, therefore, the order of the rules is also decisive for the results.
- The virus filter can only handle a limited number of simultaneous connections to mail, HTTP and FTP servers. Exceeding this number will cause further connection attempts to be refused.
- If the FTP virus filter is activated, the firewall will open the corresponding ports regardless of whether there are any firewall rules to the contrary.

You have the following options for the entries:

Server

0.0.0.0/0 means all addresses, i.e. the system will filter the traffic of all FTP servers. To enter an address space, use the CIDR notation – see “CIDR (Classless InterDomain Routing)” on page 89.

- Since an attempt to setup a connection is first handled by the proxy, if a nonexistent server is requested (e.g. a bad IP address) the user software will act as though the connection to the server had been established, but no data was sent. If the list contains the exact server addresses, this behavior can be prevented, since the proxy will then only take requests addressed to the servers given in the list.

Server Port

Enter the number of the port for the FTP protocol in this field. The default setting for the FTP port is **21**.

Comment

An informational comment for this rule.

Scan

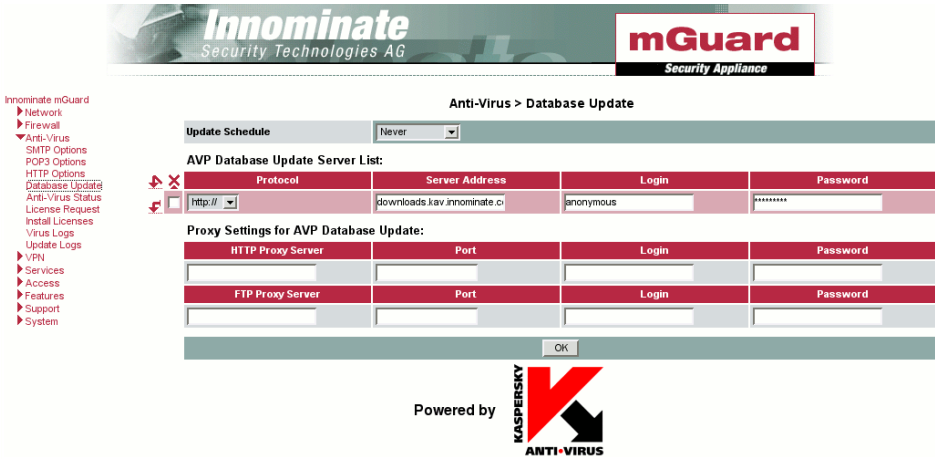
Scan

The virus filter is activated for the server specified in this rule.

No Scan

The virus filter is deactivated for the server specified in this rule.

Anti-Virus → Database Update



The virus signature files can be updated from a selected update server at intervals defined by the user. The update is performed without interrupting the operation of the anti-virus filter. The mGuard is delivered without any virus signatures installed. Therefore, after the anti-virus protection has been activated with the corresponding license, you should also set the update schedule. The course of the updates can be examined in the anti-virus Update log.

Update Schedule

This parameter is used to set how often the signature files are updated. The size of the signature file is currently about 3 MByte. The system will only download the updated files from the update server.

AVP Database Update Server List:

You can select the server from which the updated signature files should be downloaded. A default server has already been entered. If necessary, you can enter your own servers.

⌧ The list of servers will be processed from the top down until an available server is found.

☞ Inserting, moving and deleting rows is explained under “Working with tables” on page 16.

You have the following options for the entries:

Protocol

The updated virus signature files can be downloaded using either FTP or HTTP.

Server Address

In this field, enter the FQDN or IP address of the server with the full path name of the directory in which the signature file is to be found.

Login

In this field, enter the user name to be used for connecting to the server. If the update is to be made using the HTTP protocol, the login and password may need not be entered.

Password

In this field, enter the password to be used when logging in. If the update is to be made using the HTTP protocol, the login and password may need not be entered.

Proxy Settings for AVP Database Update:

When the mGuard is located behind a firewall which restricts HTTP or FTP access to use a proxy server, the following rows can be used to specify the required proxy settings.

☞ For the proxy server to be used the fields **HTTP/FTP Proxy Server** *and* **Port** must be set.

☞ To authenticate with the proxy server the fields **Login** *and* **Password** must be set.

HTTP/FTP Proxy Server

The proxy servers IP or hostname.

Port

The port belonging to the IP or hostname of the proxy server.

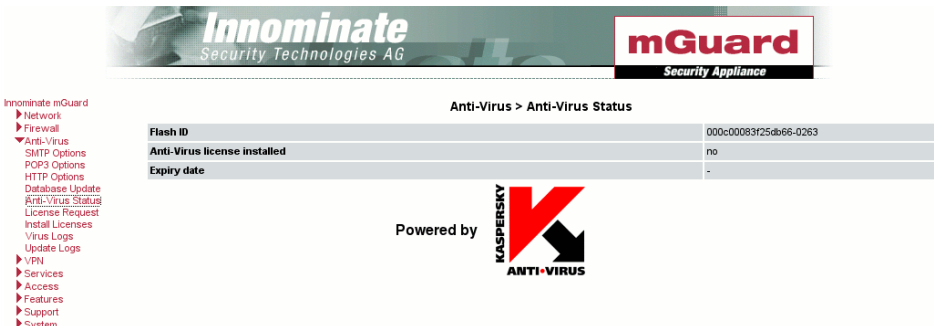
Login

The login in case the proxy server requires authentication.

Password

The password belonging to the login.

Anti-Virus → Anti-Virus Status



You can verify that the virus filter has been successfully enabled. In this menu, you will also find the date on which your license will expire.

Anti-Virus Engine Status

Displays the state of the Kaspersky scan-engine. If you have activated the anti-virus protection for at least one protocol, the status will be displayed as “up”.

Last Anti-Virus Update

Diplays the current release date of the anti-virus database.

Anti-Virus Update Status

Shows if the anti-virus update is activated or currently downloading

Anti-Virus license installed

Here you can examine the validity of the installed AVP licence.

Expiry date

Shows the expiry date of your anti-virus license.

Anti-Virus → License Request

When you purchase your anti-virus license, you will receive a voucher certificate with a license key and a license serial number. To activate your virus filter, you must enter this data in a form while requesting your license file. To open this request form, press on the corresponding button in the **Anti-Virus> License Request** menu.

The corresponding Web page will open in which you must enter the following information:

Voucher Serial Number: In this field, enter the serial number that is printed on your voucher.

Voucher Key: In this field, enter the voucher key that is printed on your voucher.

Flash ID: This value will be entered automatically.

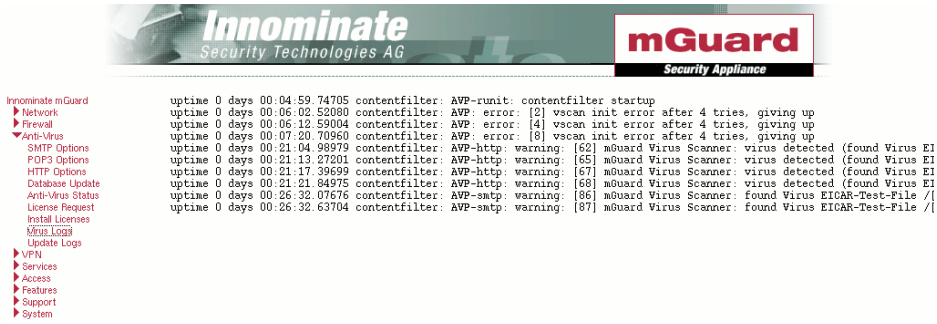
e-mail Address: In this field, enter your e-mail address. The license file will be sent to this address.

Once you have submitted the completed form, the license file will be sent to the e-mail address that you have specified.

Anti-Virus →Install license

To install the license file, open the **Anti-Virus >Install Licenses** menu, browse to the license file (so that it appears under “Filename”) and then click on the install button.

Anti-Virus → Anti-Virus Logs


Innominate
Security Technologies AG
mGuard
Security Appliance
Innominate mGuard
Network
Firewall
Anti-Virus
SMTP Options
POP3 Options
HTTP Options
Database Update
Anti-Virus Status
License Request
Install Licenses
Virus Logs
Update Logs
VPN
Services
Access
Features
Support
System
uptime 0 days 00:04:59.74705 contentfilter: AVP-runit: contentfilter startup
uptime 0 days 00:06:02.52080 contentfilter: AVP: error: [2] vscan init error after 4 tries, giving up
uptime 0 days 00:06:12.59004 contentfilter: AVP: error: [4] vscan init error after 4 tries, giving up
uptime 0 days 00:07:20.70960 contentfilter: AVP: error: [8] vscan init error after 4 tries, giving up
uptime 0 days 00:21:04.98979 contentfilter: AVP-http: warning: [62] mGuard Virus Scanner: virus detected (found Virus EI
uptime 0 days 00:21:13.27201 contentfilter: AVP-http: warning: [65] mGuard Virus Scanner: virus detected (found Virus EI
uptime 0 days 00:21:17.39699 contentfilter: AVP-http: warning: [67] mGuard Virus Scanner: virus detected (found Virus EI
uptime 0 days 00:21:21.84975 contentfilter: AVP-http: warning: [68] mGuard Virus Scanner: virus detected (found Virus EI
uptime 0 days 00:26:32.07676 contentfilter: AVP-smtp: warning: [86] mGuard Virus Scanner: found Virus EICAR-Test-File /[
uptime 0 days 00:26:32.63704 contentfilter: AVP-smtp: warning: [87] mGuard Virus Scanner: found Virus EICAR-Test-File /[

The Anti-Virus Log contains the following messages from the virus filter:

- The names of any viruses found together with the following information: name of the file and (in the case of an e-mail) the sender, date and subject.
- Warnings sent whenever the system has passed a file through unscanned because it was larger than the maximum file size.
- Program startup and shutdown.
- Error messages from the Kaspersky Scan-Engine and the virus filter.

Error Messages

Virus Detection

A virus has been detected. The error message includes the name of the virus, the sender of the e-mail, the date sent and the name of the infected file or the name of the compressed archive file and the infected portion of this archive.

An example of a virus message:

```
mGuard detected a virus. The mail could not be delivered.
found Virus Email-Worm.Win32.NetSky.q /[From
sick@example.com][Date Fri, 13 Aug 2004 11:33:53++0200]/
about_you.zip/document.txt.exe
[000012a7.00000077.00000000]
Message Details:
From: sick@example.com
Subject: Private document
Date: Fri, 13 Aug 2004 11:33:53 +0200
```

Exceeded maximum filesize
The maximum filesize set for this protocol was exceeded.
To transfer the file anyway, you can deactivate the virus filter either for the corresponding server for the course of the download or globally. Alternatively, you can set the “Action for ...exceeding the maximum message size” parameter to “Let the message/data pass unscanned” for the respective protocol.

⌦ In either case, the transferred file will not be scanned for viruses.

Temporary Virus Scanner Failure
A temporary error occurred while trying to scan a file. It is possible that the problem will be cleared if you repeat the transfer again at a later time or if you update the virus signature file.
Possible causes:

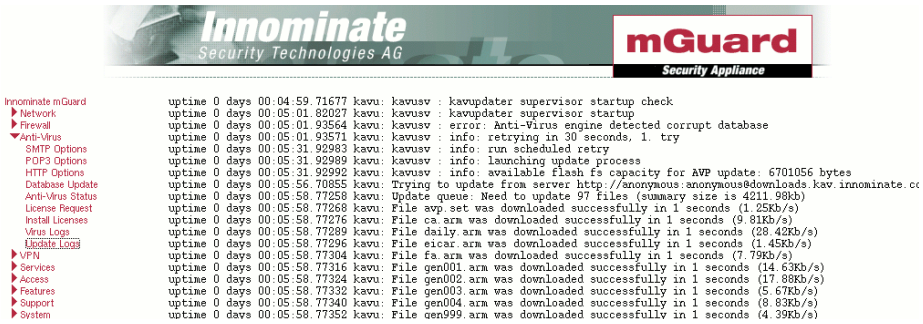
- The scan-engine cannot process the file.
- The Innominate mGuard does not have enough memory available to decompress the file.
- Internal error in the scan-engine.

Exceptional Virus Scanner Failure
A problem has occurred in the communication with the Kaspersky scan-engine. For more details, please see the anti-virus log.
Possible causes:

- The information entered for the update server is faulty and the signature update has failed (see the “Anti-Virus >Database Update” menu).
- Invalid or expired virus filter license.
- Damaged or faulty update of the virus signature file.

Update running
There is currently no anti-virus database installed, and the download of the current database has been started. You can follow the progress of the download in the anti-virus update log. After your anti-virus license expired, it may happen that the anti-virus database is deleted during a mGuard software update. After this happens, the anti-virus filter will not be useable anymore, but issue the error message “Update running”. Please deactivate the virus filter for all protocols to continue using your web browser or email client.

Anti-Virus → Anti-Virus Logs


Innominate
Security Technologies AG
mGuard
Security Appliance
Innominate mGuard
Network
Firewall
Anti-Virus
SMTP Options
POP3 Options
HTTP Options
Database Update
Anti-Virus Status
License Request
Install Licenses
Virus Logs
Update Logs
VPN
Services
Access
Features
Support
System
uptime 0 days 00:04:59.71677 kavu: kavusv : kavupdater supervisor startup check
uptime 0 days 00:05:01.82027 kavu: kavusv : kavupdater supervisor startup
uptime 0 days 00:05:01.93564 kavu: kavusv : error: Anti-Virus engine detected corrupt database
uptime 0 days 00:05:01.93571 kavu: kavusv : info: retrying in 30 seconds, 1. try
uptime 0 days 00:05:31.92983 kavu: kavusv : info: run scheduled retry
uptime 0 days 00:05:31.92989 kavu: kavusv : info: launching update process
uptime 0 days 00:05:31.92992 kavu: kavusv : info: available flash fs capacity for AVP update: 6701056 bytes
uptime 0 days 00:05:56.70855 kavu: Trying to update from server http://anonymous:anonymous@downloads.kav.innominate.c
uptime 0 days 00:05:58.77258 kavu: Update queue: Need to update 97 files (summary size is 4211.98Kb)
uptime 0 days 00:05:58.77268 kavu: File avp.set was downloaded successfully in 1 seconds (1.25Kb/s)
uptime 0 days 00:05:58.77276 kavu: File ca.arm was downloaded successfully in 1 seconds (9.81Kb/s)
uptime 0 days 00:05:58.77289 kavu: File daily.arm was downloaded successfully in 1 seconds (28.42Kb/s)
uptime 0 days 00:05:58.77296 kavu: File eicar.arm was downloaded successfully in 1 seconds (1.45Kb/s)
uptime 0 days 00:05:58.77304 kavu: File fa.arm was downloaded successfully in 1 seconds (7.79Kb/s)
uptime 0 days 00:05:58.77316 kavu: File gen001.arm was downloaded successfully in 1 seconds (14.63Kb/s)
uptime 0 days 00:05:58.77324 kavu: File gen002.arm was downloaded successfully in 1 seconds (17.88Kb/s)
uptime 0 days 00:05:58.77332 kavu: File gen003.arm was downloaded successfully in 1 seconds (5.67Kb/s)
uptime 0 days 00:05:58.77340 kavu: File gen004.arm was downloaded successfully in 1 seconds (8.83Kb/s)
uptime 0 days 00:05:58.77352 kavu: File gen999.arm was downloaded successfully in 1 seconds (4.39Kb/s)

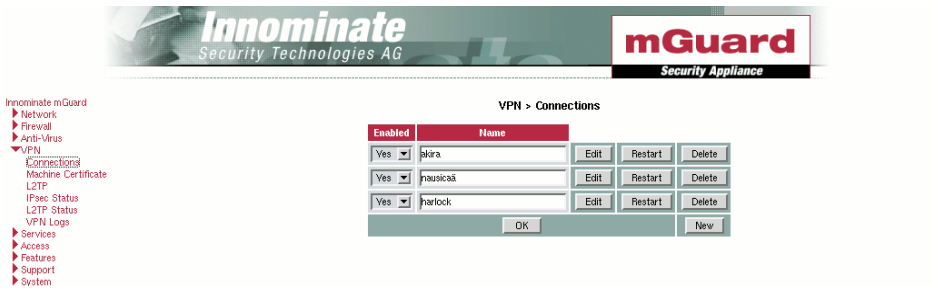
The update log contains messages about the start and course of virus signature updates.

5.9 VPN Menu

Prerequisites for a VPN connection:
The main prerequisite for a VPN connection is that the IP addresses of the VPN partner are known and accessible.

- In order for an IPsec connection to be setup successfully, the VPN's remote site must support IPsec with the following configuration:
  – Authentication via Pre-Shared Key (PSK) or X.509 certificate
  – ESP
  – Diffie-Hellman Groups 2 and 5
  – DES, 3DES or AES encryption
  – MD5 or SHA-1 hash algorithms
  – Tunnel or Transport mode
  – Quick Mode
  – Main Mode
  – SA Lifetime (1 second to 24 hours)
  If the system at the remote site is running Windows 2000, the *Microsoft Windows 2000 High Encryption Pack* or at least *Service Pack 2* must be installed.
- If the remote site is behind a NAT router, it must support NAT-T. Or the NAT router must support the IPsec protocol (IPsec/VPN Passthrough). In either case, for technical reasons, only IPsec Tunnel connections are supported.

VPN → Connections



Lists the VPN connections that have been set up.

☞ You can activate (Enable = **Yes**) or deactivate (Enable = **No**) each individual connection.

VPN connections - deleting

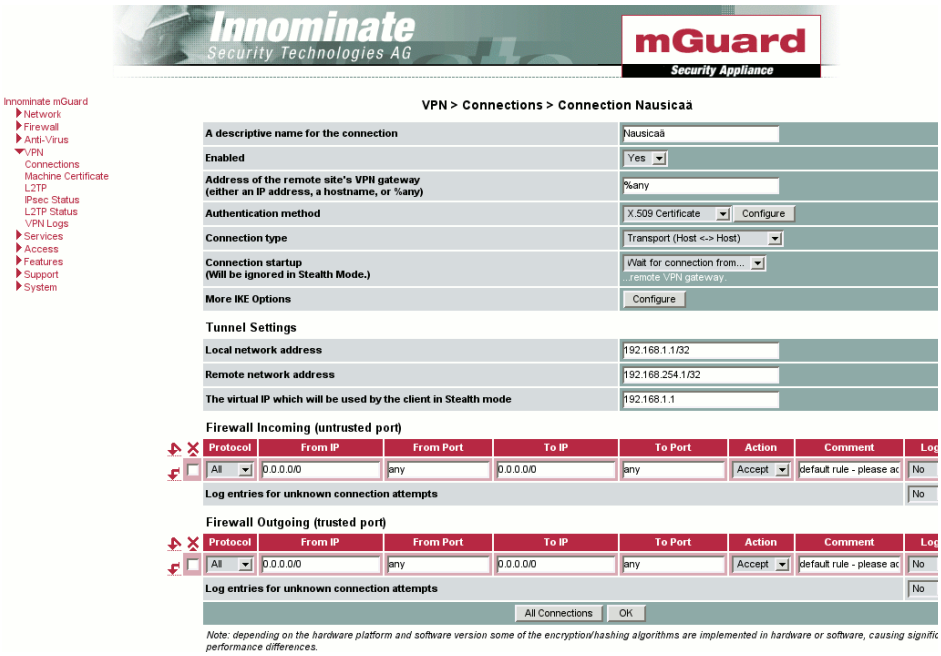
☞ Click on the **Delete** button next to the entry.
Then click on **OK**.

Configuring a new VPN connection

☞ Click on **New**.
Enter a name for the connection and then click on **Edit.**
Make the necessary or desired settings (see below).
Then click on **OK**.

VPN connections - editing

☞ Click on the **Edit** button next to the entry.
Make the necessary or desired settings (see below).
Then click on **OK**.



A descriptive name for the connection

You can assign the connection any name you desire.

Enabled

Specify whether the connection should be enabled (= Yes) or not (= No).

Address of the remote site's VPN gateway

The address of the gateway to the private network in which the remote communication partner can be found.

– If you wish to have the mGuard actively initiate and set up the connection to the remote site or if the device is in *Stealth* mode, enter the IP address of the remote site here. Instead of entering an IP address, you can enter a host name (i.e. a domain name in the URL syntax – vpn.example.com).
– If the remote site's VPN gateway does not have a fixed and known IP address, you can use the DynDNS Service to simulate a fixed and known address. See "Dienste ‡ DynDNS Registrierung" on page 71.
– If you want the mGuard to be ready to accept a connection actively initiated and set up by a remote site with any IP address, enter: **%any**
– In this case, the local mGuard can be "called" by a remote site, which has been dynamically assigned its IP address (by the internet service provider), which has an IP address that changes. In this scenario, you may only enter an IP address when this is the fixed and known IP address of the remote "calling" site.

⌦ **%any** can only be used along with the authentication mode using X.509 certificates.

⌦ In case the remote peer is located behind a NAT gateway, **%any** must be used. Otherwise the renegotiation of new connection keys will fail after the connection is established.

Authentication method

There are 2 options:

– X.509 Certificate

– Pre-Shared Key

X.509 Certificate

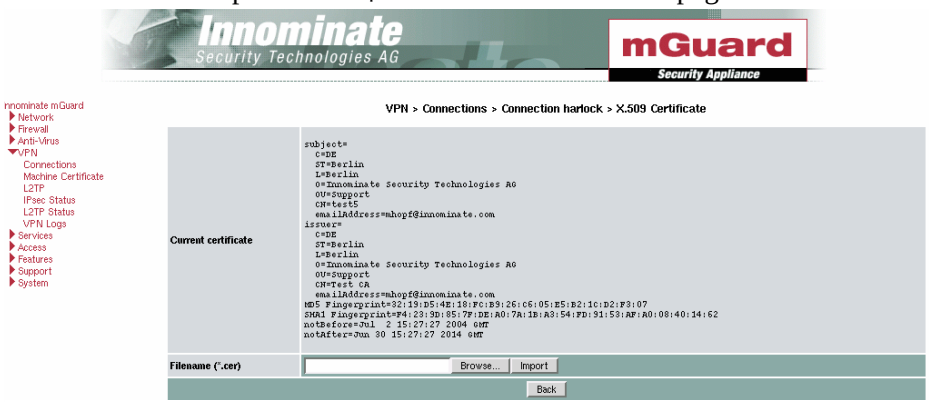
These methods are supported by most of the newer IPsec implementations. In this case, the mGuard uses the public key of the remote site (filename *.cer or *.pem) to encrypt the authentication datagram before it sends it to the remote site, the “tunnel end”. (You must have received this *.cer or *.pem file from the operator at the remote site – perhaps on a floppy disc or attached to an e-mail).

To make this public key available to the mGuard, proceed as follows:

Prerequisite:

The *.cer or *.pem file must have been saved on the configuration system.

1. Click on **Configure**.
   Afterwards: The *VPN > Connections > Connection xyz > X.509 Certificate* screen will be displayed. (“*xyz*” is the name of the respective connection.)
2. Click on **Browse...** and select the file.
3. Click on **Import**.
   After the import, the contents of the new certificate will be displayed - see the illustration below. An explanation of the information displayed can be found in the chapter “VPN ‡ Machine Certificate” on page 58.



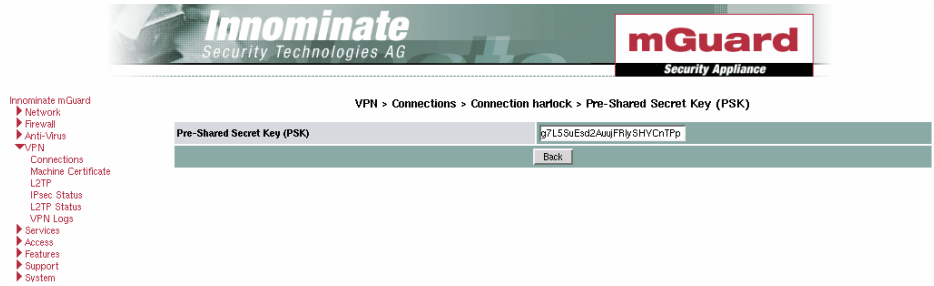
4. Click on **Back**.

Pre-Shared Secret Key (PSK)

This method is mainly used by older IPsec implementations. In this case both sides of the VPN authenticate each other with the same PSK.

To make the agreed upon key available to the mGuard, proceed as follows:

1. Click on **Configure**.
   Afterwards: The screen shown below will be displayed.



2. Enter the agreed upon character string in the *Pre-Shared Secret Key (PSK)* entry field. To achieve security comparable to that of 3DES, the string should consist of about 30 characters selected at random and should include upper

and lower case characters and digits.

3. Click on **Back**.

☞ The *Pre-Shared Secret Key* cannot be used with dynamic (%any) IP addresses; fixed IP addresses or host names are required at both ends.

Connection type

You can choose from:
Tunnel (Net[work] ←→ Net[work])
Transport (Host ←→ Host)
Transport (L2TP Microsoft Windows)
Transport (L2TP SSH Sentinel)

Tunnel (Net[work] ←→ Net[work])

This type of connection is not only suitable in every case, but also the most secure. In this mode, the IP datagrams are completely encrypted before they are sent with a new header to the remote site's VPN gateway – the "tunnel end". There the transferred datagrams are decrypted to restore the original datagrams. These are then passed on to the destination system.

Transport (Host ←→ Host)

In this type of connection, the device only encrypts the data of the IP packets. The IP header information remains unencrypted.

Transport (L2TP Microsoft Windows)

If this type of connection is activated on the remote system, the mGuard will use *Transport (L2TP Microsoft Windows)*. In this case, the mGuard will function accordingly. In other words, the L2TP/PPP protocol will create a tunnel within the IPsec transport connection. The locally connected L2TP system will be assigned its IP address dynamically by the mGuard.
If you select the connection type *Transport (L2TP Microsoft Windows)*, set *Perfect Forward Secrecy (PFS)* to **No** (see below). Also enable the L2TP server.

☞ As soon as the IPsec/L2TP connection is started under Windows, a dialog will appear to prompt you to enter your user name and login. You can make any entry that you want in this dialog. Since the X.509 certificate has already provided your authentication, the mGuard will ignore these entries.

Transport (L2TP SSH Sentinel)

If this type of connection is activated with a locally connected system, set *Transport (L2TP SSH Sentinel)* on the mGuard as well. In this case, the mGuard will function accordingly. In other words, the L2TP/PPP protocol will create a tunnel within the IPsec transport connection. The locally connected L2TP system will be assigned its IP address dynamically by the mGuard. Also enable the L2TP server.

Connection startup

There are 2 options:

- Start a connection to the remote side
- Wait for the remote side [to setup a connection]

Start a connection to the remote side

In this case, the local mGuard sets up the connection to the remote side. The fixed IP address or domain name of the remote side must be entered in the *Address of the remote site's VPN gateway* (see above) field.

Wait for the remote side [to setup a connection]

In this case, the local mGuard is ready to accept a connection, which a remote site actively initiates and sets up to the local mGuard. The entry in the *Address of the remote site's VPN gateway* (see above) field may be: **%any**

If the mGuard should only accept a connection initiated by a specific remote site (which has a fixed IP address), you can enter its IP address or hostname just to be on the safe side.

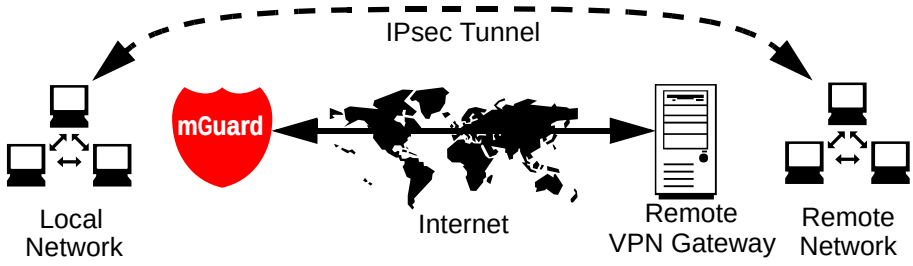
☞ If the mGuard is running in *Stealth* mode, this setting has no effect. In other words, it will be ignored and the connection will be initiated automatically, whenever the mGuard notices that the connection should be used.

More IKE Options

Click on **Configure** to define more advances IKE options like encryption algorithms, Key Lifetimes or Dead Peer Detection (DPD). Full details are given below.

Tunnel Settings

When the *Connection Type* is set to "Tunnel", the following entries must be specified:



Local network address

With this entry, you specify the address of the network or computer which is connected to the local interface of the mGuard.

Remote network address

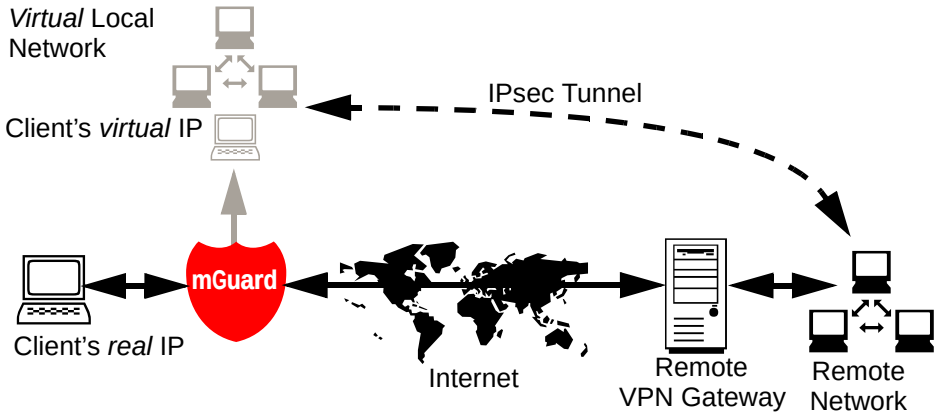
With this entry, you specify the address of the network or computer which is available behind the remote VPN gateway.

☞ The network 0.0.0.0/0 specifies a *default route over the VPN*.

This means that all traffic for which there is no other VPN tunnel or route will be routed through this VPN tunnel.

A default route over VPN should only be specified for a single tunnel and is not available in *Stealth* mode.

The virtual IP which will be used by the client in stealth mode



In *Stealth* mode the VPN's local network is simulated by the mGuard. Inside this *virtual* network, the client will be known under a *virtual IP*.

⌦ This entry is only required in *Stealth* mode.

Firewall incoming, Firewall outgoing

While the settings made in the *Firewall* menu only affect non-VPN connections (see above under "Firewall ‡ Incoming" on page 27), these settings affect just the VPN connection defined here. This means: If you have defined multiple VPN connections, you can restrict the outgoing or incoming access individually for each connection. You can have any attempts made to bypass these restrictions logged.

⌦ The VPN Firewall factory settings allow all connections via this VPN connection.
However, the extended settings (defined and described earlier - see "Firewall ‡ Extended Settings" on page 33) do apply independently for each individual VPN connection.

⌦ If multiple firewall rules are set, they will be searched in the order in which they are listed from top to bottom until a suitable rule is found. This rule will then be applied. If further down in the list there are other rules which would also fit, they will be ignored.

⌦ In stealth mode the firewall rules the real IP address is to be used for the client or left at 0.0.0.0/0, as only one client can be addressed through the tunnel.

☞ Inserting, moving and deleting rows is explained under "Working with tables" on page 16.

As in the previous sections, you have the following options when making the entries:

Protocol

All means: TCP, UDP, ICMP and other IP protocols.

From IP/To IP

0.0.0.0/0 means all addresses. To enter an address space, use the CIDR notation – see "CIDR (Classless InterDomain Routing)" on page 89.

From Port/To Port

(This is only evaluated by the TCP and UDP protocols)

any means each and every port.

startport:endport (e.g. 110:120) defines a range of ports.

You can specify individual ports by giving either their port number or the corresponding service name: (e.g. 110 for pop3 or pop3 for 110).

Action

Accept means that the data packets should be passed through.

Reject means that the data packets should be rejected so that the sender is informed that the data packets have been rejected. (In *Stealth* mode, Reject has the same effect as Drop (see below).)

Drop means that the data packets should not be passed through. The data packets will be discarded so that the sender will not be informed as to what happened to them.

Comment

An informational comment for this rule.

Log

You can specify - for each individual firewall rule - whether the use of the rule

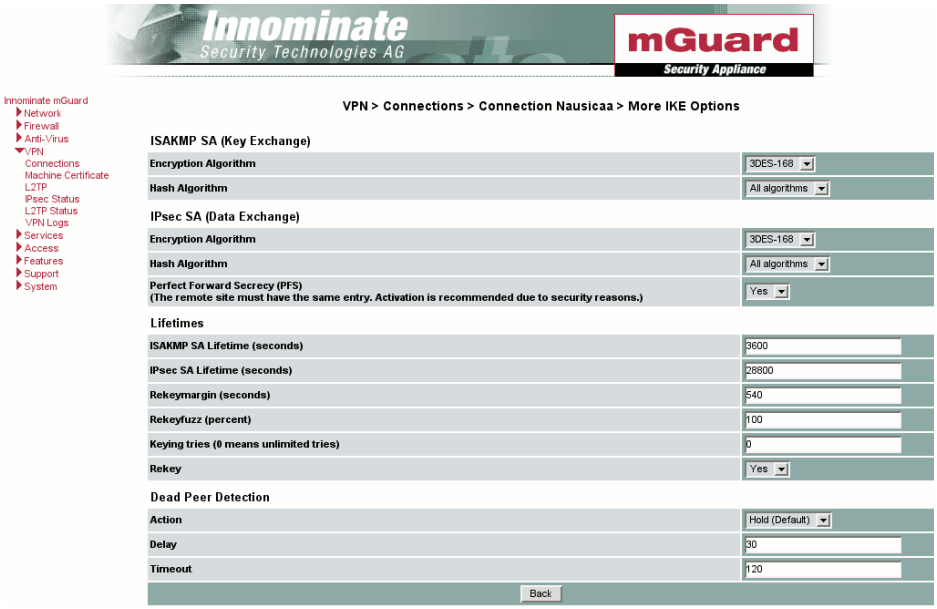
☞ should be logged by setting - *Log* to **Yes**

☞ or not by setting - *Log* to **No** (factory setting).

Log entries for unknown connection attempts

If this is set to Yes, all attempts to establish a connection, which were not covered by the rules defined above, will be logged.

More IKE Options



ISAKMP SA (Key Exchange)

Encryption algorithm

☞ Together with the administrator at the remote site, decide on which encryption technique should be used.

3DES-168 is the most commonly used algorithm and is therefore the default (factory) setting.

Basically the following applies: The greater the number of bits used by an encryption algorithm - specified by the appended number -, the more secure it is. The relatively new AES-256 protocol is therefore considered the most secure, but is not yet widely used.

The longer the key, the longer the time required by the encryption process. This latter point, however, is of no consequence for the mGuard, since it uses a hardware-based encryption technique. However, this aspect may be of significance for the remote site.

The algorithm designated as “Null” performs no encryption.

Hash Algorithm

Leave this setting on *All algorithms*. With this setting, it is does not matter whether the remote site uses MD5 or SHA-1.

IPsec SA (Data Exchange)

In contrast to *ISAKMP SA (Key Exchange)* (see above), this setting determines the method used for the exchange of data. This may be different from the Key Exchange but need not be.

Encryption Algorithm

See above

Hash Algorithm

See above

Perfect Forward Secrecy (PFS)

This method is used to increase the security of the data transfer. In IPsec, the key used for the data exchange is changed at certain intervals. In the case of PFS, a new random number is negotiated with the remote site instead of deriving it from a previously agreed on random number.

☞ Do not set this to **Yes**, unless the remote site also supports PFS.

If you select the connection type *Transport (L2TP Microsoft Windows)*, set *Perfect Forward Secrecy (PFS)* to **No**.

Lifetimes

The keys of an IPsec connection will be renegotiated at certain intervals to increase the costs of an attack at the IPsec connection.

ISAKMP SA Lifetime

The lifetime of the ISAKMP SA keys in seconds.

The factory default is 3600 seconds (1 hour). The allowed maximum is 28800 seconds (8 hours).

IPsec SA Lifetime

The lifetime of the IPsec SA keys in seconds.

The factory default is 28800 seconds (8 hours). The allowed maximum is 86400 seconds (24 hours).

Rekeymargin

Minimal time interval before the old key expires during which a new key shall be negotiated. The factory default is 540 seconds (9 minutes).

Rekeyfuzz

Maximum in percent by which *Rekeymargin* shall be randomly increased.

This is to lower the load during key exchanges on machines with many VPN connections by serializing them. The factory default is 100 percent.

Keying tries

Number of attempts to negotiate new keys with the remote peer.

The special value 0 means unlimited attempts in case the connection is to be initiated by the mGuard, otherwise it means 5.

Rekey

When set to **Yes**, this side will try to renegotiate keys when they expire.

Dead Peer Detection

When the remote peer supports the Dead Peer Detection (DPD) protocol, both peers can detect whether the connection is still valid or must be renegotiated. Without DPD, the connection must be either restarted manually or is unusable until the initiating sides SAs expire.

Action

When set to **Hold**, a connection found dead will be renegotiated. When set to **Clear**, the keys are cleared and the connection stays down.

The factory default is **Hold**.

Delay

The length of time in seconds after which DPD Keep Alive queries will be sent to check the availability of the remote peer.

The factory default is 30 seconds.

Timeout

The length of time in seconds after which the remote peer will be declared dead if the Keep Alive queries are not answered.

The factory default is 120 seconds.

VPN → Machine Certificate

Certificate

This shows the currently imported X.509 certificate with which the mGuard identifies itself to other VPN gateways. The following information is displayed:

subject	The holder to whom the certificate was issued.
issuer	The certification authority which signed the certificate. C: Country ST: State L: Location (city) O: Organisation OU: Organisation Unit CN: Common Name (hostname)
MD5, SHA1 Fingerprint	Fingerprint of the certificate to compare this with another person, e.g. on the telephone. Windows displays the fingerprint in SHA1 format here.
notBefore, notAfter	Period of time that the certificate is valid. This is ignored by the mGuard, since it doesn't have an integrated realtime clock.

In addition to the information given above, the imported certificate file (filename extension *.p12 or *.pfx) also contains the two keys - the public key to encrypt data and the private key to decrypt it. The associated public key can be shared with any number of parties to enable them to decode the encrypted data. Depending on the respective remote site, its operator must be supplied the

certificate in the form of a *.cer or *.pem file – for example, in person or via an e-mail. If a secure means of communication is not available, you should conclude by comparing the fingerprint shown by the mGuard via a secure means.

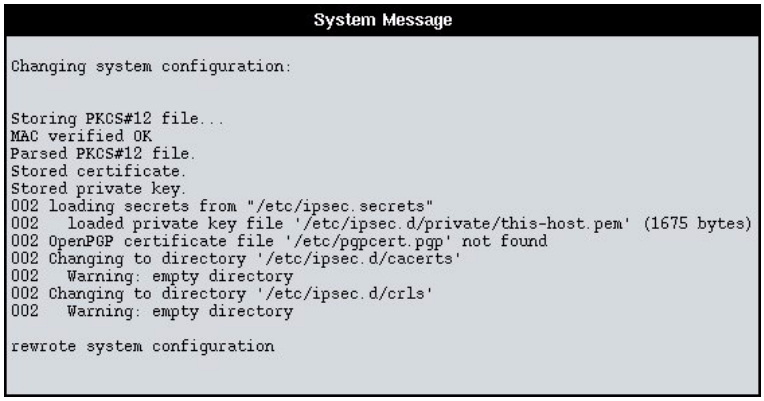
Only one certificate file (PKCS#12 file) can be imported into the device.
To import a (new) certificate, proceed as follows:

New Certificate

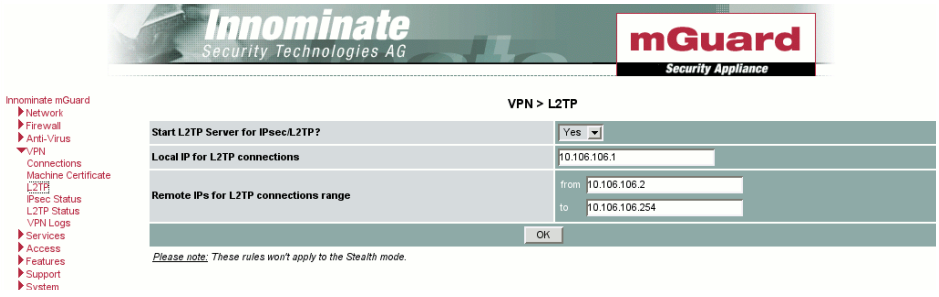
Prerequisite:

The certificate file (filename = *.p12 or *.pfx) is generated and saved on the connected system.

1. Click on **Browse...** to select the file.
2. Enter the password with which the PKCS#12 file's private key is protected in the *Password* field.
3. Click on **Import**.
4. Then click on **OK**.
   After the import is completed, the following system message will be displayed:


System Message
Changing system configuration:
Storing PKCS#12 file...
MAC verified OK
Parsed PKCS#12 file.
Stored certificate.
Stored private key.
002 loading secrets from "/etc/ipsec.secrets"
002 loaded private key file '/etc/ipsec.d/private/this-host.pem' (1675 bytes)
002 OpenPGP certificate file '/etc/pgpcert.pgp' not found
002 Changing to directory '/etc/ipsec.d/cacerts'
002 Warning: empty directory
002 Changing to directory '/etc/ipsec.d/crls'
002 Warning: empty directory
rewrote system configuration

VPN → L2TP (mGuard smart enterprise only)



Start L2TP Server for IPsec/L2TP? Yes / No

If you want to enable IPsec/L2TP connections, set this switch to **Yes**. It is then possible to establish incoming L2TP connections over IPsec, which dynamically assign IP addresses to the clients within the VPN.

Local IP for L2TP connections

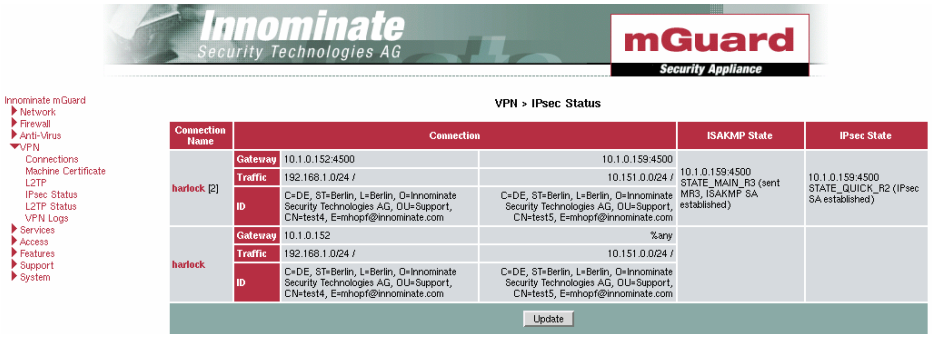
With the setting shown in the screenshot above, the mGuard will inform the remote site that the mGuard's address is 10.106.106.1.

Remote IPs for L2TP connections range

With the settings shown in the screenshot above, the mGuard will assigned IP addresses between 10.106.106.2 and 10.106.106.254 to the remote peers.

VPN → IPsec Status

Display only:



Shows the status of the IPsec connections.
The names of the VPN connections are listed on the left. On the right, you will find the current status of each connection.

GATEWAY
shows the IP addresses of the communication VPN gateway

TRAFFIC
identifies the systems or networks which communicate via the VPN gateways.

ID
identifies the Distinguished Name (DN) of an X.509 certificate.

ISAKMP State
ISAKMP State (Internet security association and key management protocol) is given as “established”, if the two VPN gateways involved have established a channel to exchange keys. In this case, they have been able to contact each other and all of the settings made on the configuration page up to and including “ISAKMP SA” were correct.

IPsec State
IPsec State is given as “established”, if IPsec encryption is activated when communicating. In this case, the entries made under “IPsec SA” and “Tunnel Settings” were also correct.

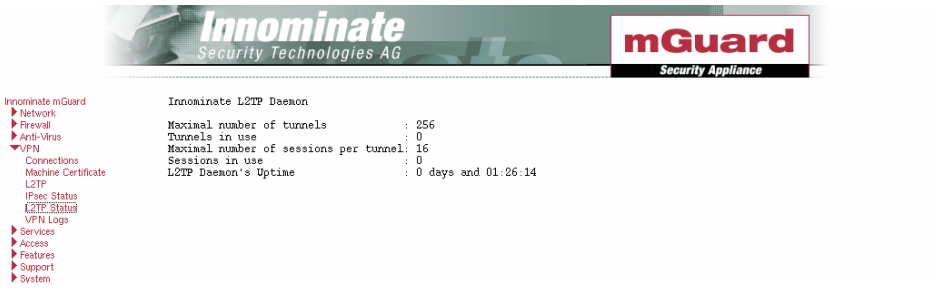
In the event of problems, we recommend that you examine the VPN log of the system to which the connection was setup. The basis for this recommendation is that for reasons of security exhaustive error messages are not returned to the initiating system.

If the display shows:
ISAKMP SA established, IPsec State: WAITING
This indicates that:
the authentication was successful, but the other parameters are not correct: Do the connection types (Tunnel, Transport) match? If Tunnel has been selected, do the network address areas match at both ends?

If the display shows:
IPsec State: IPsec SA established
This indicates that:
the VPN connection has been successfully setup and can be used. If this is not the case, there must be a problem with the remote VPN gateway. In this case, disable and enable the connection to re-establish the connection.

VPN → L2TP Status (mGuard smart enterprise only)

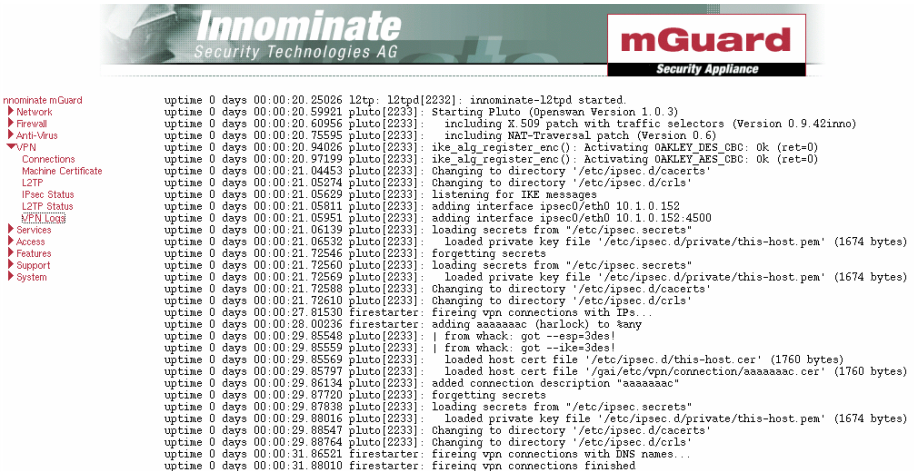
Display only:



Shows information about the L2TP status, when this type of connection has been selected. See “VPN ‡ Connections” on page 50.
If this type of connection has not been selected, the screen shown above will be displayed.

VPN → VPN Logs

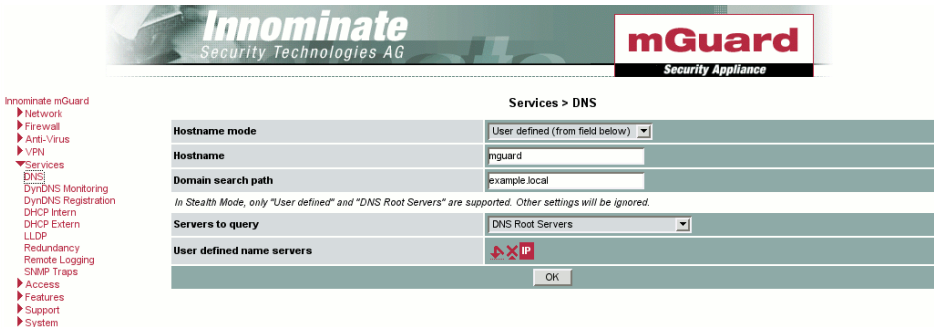
Display only:


Innominate
Security Technologies AG
mGuard
Security Appliance
innominate mGuard
Network
Firewall
Anti-Virus
VPN
Connections
Machine Certificate
L2TP
IPsec Status
L2TP Status
VPN Logs
Services
Access
Features
Support
System
uptime 0 days 00:00:20.25026 l2tp: l2tpd[2232]: innominate-l2tpd started.
uptime 0 days 00:00:20.59921 pluto[2233]: Starting Pluto (Openswan Version 1.0.3)
uptime 0 days 00:00:20.60956 pluto[2233]: including X.509 patch with traffic selectors (Version 0.9.42inno)
uptime 0 days 00:00:20.75595 pluto[2233]: including NAT-Traversal patch (Version 0.6)
uptime 0 days 00:00:20.94026 pluto[2233]: ike_alg_register_enc(): Activating OAKLEY_DES_CBC: Ok (ret=0)
uptime 0 days 00:00:20.97199 pluto[2233]: ike_alg_register_enc(): Activating OAKLEY_AES_CBC: Ok (ret=0)
uptime 0 days 00:00:21.04453 pluto[2233]: Changing to directory '/etc/ipsec.d/cacerts'
uptime 0 days 00:00:21.05274 pluto[2233]: Changing to directory '/etc/ipsec.d/crls'
uptime 0 days 00:00:21.05629 pluto[2233]: listening for IKE messages
uptime 0 days 00:00:21.05811 pluto[2233]: adding interface ipsec0/eth0 10.1.0.152
uptime 0 days 00:00:21.05951 pluto[2233]: adding interface ipsec0/eth0 10.1.0.152:4500
uptime 0 days 00:00:21.06139 pluto[2233]: loading secrets from "/etc/ipsec.secrets"
uptime 0 days 00:00:21.06532 pluto[2233]: loaded private key file '/etc/ipsec.d/private/this-host.pem' (1674 bytes)
uptime 0 days 00:00:21.72546 pluto[2233]: forgetting secrets
uptime 0 days 00:00:21.72560 pluto[2233]: loading secrets from "/etc/ipsec.secrets"
uptime 0 days 00:00:21.72569 pluto[2233]: loaded private key file '/etc/ipsec.d/private/this-host.pem' (1674 bytes)
uptime 0 days 00:00:21.72588 pluto[2233]: Changing to directory '/etc/ipsec.d/cacerts'
uptime 0 days 00:00:21.72610 pluto[2233]: Changing to directory '/etc/ipsec.d/crls'
uptime 0 days 00:00:27.81530 firestarter: fireing vpn connections with IPs...
uptime 0 days 00:00:28.00236 firestarter: adding aaaaaaac (hardlock) to %any
uptime 0 days 00:00:29.85548 pluto[2233]: | from whack: got --esp=3des!
uptime 0 days 00:00:29.85559 pluto[2233]: | from whack: got --ike=3des!
uptime 0 days 00:00:29.85569 pluto[2233]: loaded host cert file '/etc/ipsec.d/this-host.cer' (1760 bytes)
uptime 0 days 00:00:29.85797 pluto[2233]: loaded host cert file '/gai/etc/vpn/connection/aaaaaaac.cer' (1760 bytes)
uptime 0 days 00:00:29.86134 pluto[2233]: added connection description "aaaaaaac"
uptime 0 days 00:00:29.87720 pluto[2233]: forgetting secrets
uptime 0 days 00:00:29.87838 pluto[2233]: loading secrets from "/etc/ipsec.secrets"
uptime 0 days 00:00:29.88016 pluto[2233]: loaded private key file '/etc/ipsec.d/private/this-host.pem' (1674 bytes)
uptime 0 days 00:00:29.88547 pluto[2233]: Changing to directory '/etc/ipsec.d/cacerts'
uptime 0 days 00:00:29.88764 pluto[2233]: Changing to directory '/etc/ipsec.d/crls'
uptime 0 days 00:00:31.86521 firestarter: fireing vpn connections with DNS names...
uptime 0 days 00:00:31.88010 firestarter: fireing vpn connections finished

Lists all VPN events.
The format of the log corresponds to that common under Linux.
Special analysis programs are available which can be used to present the information from the log in a more readable format.

5.10 Services Menu

Services → DNS



If the mGuard should establish a connection to a remote site (e.g. as a VPN gateway or NTP server), it must know the IP address of this remote site. If you supply this in the form of a hostname (i.e. given in the format www.example.com), the device must access a Domain Name Server (DNS) to determine which IP address is associated with this hostname.
If the mGuard is not in *Stealth* mode, you can configure the locally connected client systems to use the mGuard to retrieve the IP address associated with a hostname. See “IP configuration on Windows clients” on page 66

Hostname mode

Using the *Hostname mode* and *Hostname* fields, you can assign a name to the mGuard. This will then be displayed, e.g. when logging in via SSH. The administration of multiple mGuards is simplified if you assign hostnames to them.

User defined (see below)

(Default) The name entered in the *Hostname* field is assigned to the mGuard.

☞ If the mGuard is running in *Stealth* mode, the option *User defined* must be selected under *Hostname mode*.

Provider defined (e.g. via DHCP)

If the selected network mode permits the external setting of the hostname e.g. via DHCP, the name received from the provider will be assigned to the mGuard.

Hostname

If the option *User defined* is selected under *Hostname mode*, enter the name which should be assigned to the mGuard here.
Otherwise, i.e. if the option *Provider defined (e.g. via DHCP)* is selected under *Hostname mode*, the entry in this field will be ignored.

Domain search path

This entry makes it easier for the user to specify a domain name: If the user enters the domain name in an abbreviated form, the mGuard will extend the entry by appending the domain suffix, which is defined here in the *Domain search path*.

Servers to query

Possible settings:

- DNS Root Servers
- Provider defined (i.e. via PPPoE or DHCP)
- User defined (servers listed below)

DNS Root Servers:

Queries will be sent to the DNS Root server in Internet found at the IP address which is stored in the mGuard. These addresses rarely change.

Provider defined (e.g. via PPPoE or DHCP)

With this setting, the device will use the Domain Name Server of the Internet Service Provider, which is used to access the Internet. Only select this setting if the mGuard is operated in *PPPoE* or *PPTP* mode or in *Router* mode with DHCP.

User defined (servers listed below)

If this setting is selected, the mGuard will connect to the Domain Name Servers shown in the list of *User defined name servers*.

User defined name servers

You can record the IP addresses of domain name servers in this list. If one of these should be used by the mGuard, select the option **User defined (servers listed below)** under *Servers to query*.

☞ Inserting, moving and deleting rows is explained under “Working with tables” on page 16.

Services → DynDNS Monitoring

For an explanation of DynDNS, see below: Services → DynDNS Registration.

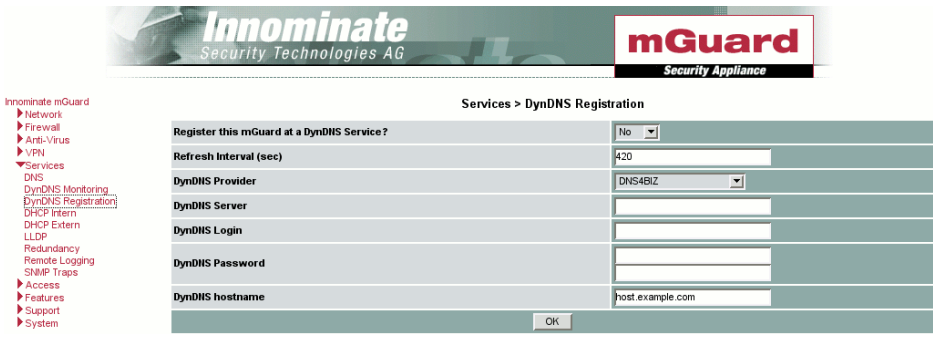
Watch hostnames of remote VPN Gateways? Yes / No

If the mGuard has been given the address of the remote VPN gateway as a hostname (see “VPN ‡ Connections” on page 50) and this hostname has been registered with a DynDNS Service, the mGuard can check against the DynDNS at regular intervals whether any changes have occurred. If yes, the VPN connection will be setup to the new IP address.

Refresh Interval (sec)

Standard: 300 (seconds)

Services → DynDNS Registration



If a VPN connection is to be setup, at least the IP address of one of the partners must be known so that the other can setup a connection to it. This condition is not satisfied, if both sites/stations are assigned their IP addresses dynamically by their respective Internet Service Providers. In this case, a DynDNS-Service such

as DynDNS.org or DNS4BIZ.com can be of assistance. The currently valid IP address of a site/station is registered under a fixed name at a DynDNS service. If you have registered with one of the DynDNS services supported by mGuard, you can enter the corresponding information in this screen.

Register this mGuard at a DynDNS Service? Yes / No

Select **Yes**, if you have registered with a DynDNS provider and the mGuard should utilize this service. In this case, the mGuard will report its current IP address – the one assigned for its own Internet access by its Internet Service Provider – to the DynDNS Service.

Refresh Interval (sec)

Standard: 420 (seconds)

Whenever the IP address of its own Internet access is changed, the mGuard will inform the DynDNS Service of its new IP address. For additional reliability, the device will also report its IP address at the interval set here.

This setting is ignored for some DynDNS providers like DynDNS.org where too many updates will cause the account to be closed.

DynDNS Provider

The providers in the list support the same protocol as the mGuard.

Select the name of the provider with which you are registered, e.g. DynDNS.org.

DynDNS Server

The name of the server of the DynDNS provider selected above, e.g.: dyndns.org.

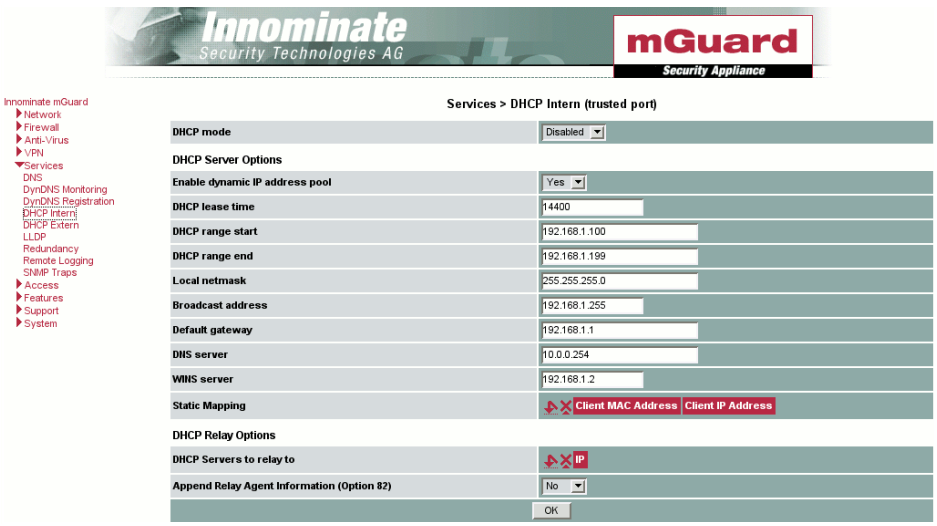
DynDNS Login, DynDNS Password

Enter the user name and password that you have been assigned by the DynDNS provider here.

DynDNS Hostname

The name selected at the DynDNS Service for this mGuard - if you use a DynDNS Service and have entered the corresponding data above.

Services → DHCP Intern/Extern



The Dynamic Host Configuration Protocol (DHCP) automatically assigns appropriate network parameters (like IP address or subnet mask) to the clients connected to the mGuard. Under *DHCP Intern* you can configure the settings for the internal interface (LAN) and under *DHCP Extern* the settings for the external interface (WAN).

DHCP mode

Server

The mGuard will work as an independent DHCP server.

Relay

The mGuard will forward DHCP requests to other DHCP servers on its external interface (WAN).

Disabled

The mGuard will not answer DHCP requests.

⌧ The DHCP server/relay is also operational in stealth mode.

DHCP server options

Enable dynamic IP address pool

Select **Yes**, if you wish to use the dynamic IP address pool defined by **DHCP range start** and **DHCP range end**.

Select **No**, if you wish to use IP addresses statically assigned by the means of the MAC address (see below).

DHCP lease time

Time in seconds, for which the network configuration assigned to the client is valid. Briefly before expiration of this time the client should renew its configuration. Otherwise it may be assigned to another computer.

Options:

When the DHCP server and the dynamic IP address pool has been activated, you can enter the network parameters that should be used by the client(s):

DHCP range start: **DHCP range end:**	The start and end of the address range from which the mGuard's DHCP server should assign IP addresses to its locally connected clients.
Local Netmask:	The factory setting is: 255.255.255.0
Broadcast IP:	The clients broadcast IP.
Default gateway:	This field is used to define which IP address should be used by the client(s) as the standard gateway. Usually this is the local IP address of the mGuard.
DNS server:	This field is used to define the Domain Name Service (DNS) server which the clients can access to find out the IP address that is associated with a specific domain name.
WINS-server:	This field is used to define the Windows Internet Naming Service (WINS) server.

Static mapping

You can find out the MAC address of your client by using the following commands:

Windows 95/98/ME: Click on the **Start** button, and then click on **Run**. Type **winipcfg** in the Open box, and then click on **OK**. The MAC address will be shown as “Adapter Address”
NT/2000/XP: Select the **Start** button on the Task Bar. Select **Run**. Type **cmd.exe**. When the DOS command prompt window opens, type **ipconfig /all** The MAC address will be shown as “Physical Address”.
Linux: Start **/sbin/ifconfig** or **ip link show** in a shell.

☞ Inserting, moving and deleting rows is explained under “Working with tables” on page 16.

You must enter the following data when assigning IP and MAC addresses:

Client MAC address
The MAC address of the client. Please enter without spaces or hyphens.

Client IP address
The IP address you wish to assign to the MAC address.

☞ The statically assigned IP addresses take priority over the dynamic IP address pool

☞ Static IP addresses and pool addresses must not overlap

☞ Do not assign one IP address to several MAC addresses, otherwise several clients will be assigned the same IP address

☞ You should only use one DHCP server per subnetwork.

DHCP relay options

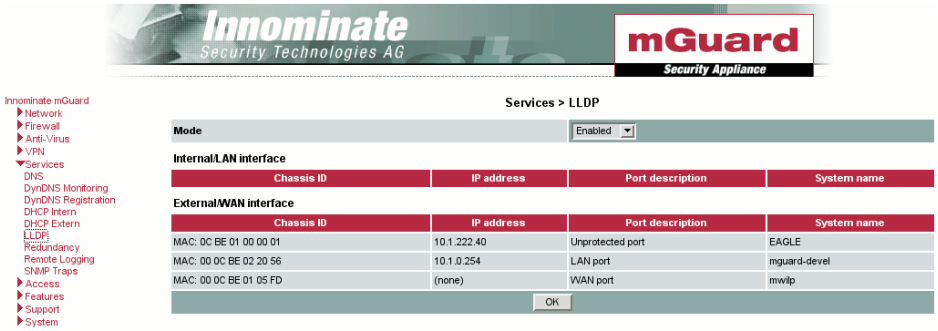
DHCP servers to relay to
A list of DHCP servers, to which DHCP requests are to be passed on.

Append Relay Agent Information
When this option is set to **Yes**, additional information according to RFC 3046 will be added.

⌦ IP configuration on Windows clients
If you start the mGuard’s DHCP server, you can configure the locally connected clients to retrieve their IP addresses automatically.

To do so, if you are using Windows XP, click on **Start, Control Panel, Network Connections**: Right click on the icon of the LAN adapter and then click on **Properties** in the pop-up menu. In the *Internet Protocol Properties* dialog on the *General* tab, select **Internet Protocol (TCP/IP)** under "This connection uses the following items" and then click on the **Properties** button. In the *Internet Protocol Properties (TCP/IP)* dialog, make the appropriate entries or settings.

Services → LLDP (mGuard smart enterprise only)



LLDP (Link Layer Discovery Protocol, IEEE 802.1AB) supports the automatic detection of the (ethernet) network topology.
LLDP capable devices periodically send ethernet multicasts (layer 2) with network information about themselves which will be collected by other LLDP capable devices and made available via SNMP.

Mode

Enabling and disabling of the LLDP service.

Internal/LAN interface and External/WAN interface

Chassis ID

An entity which identifies a remote device uniquely; typically one of its MAC addresses.

IP address

The IP address to manage the remote device via SNMP.

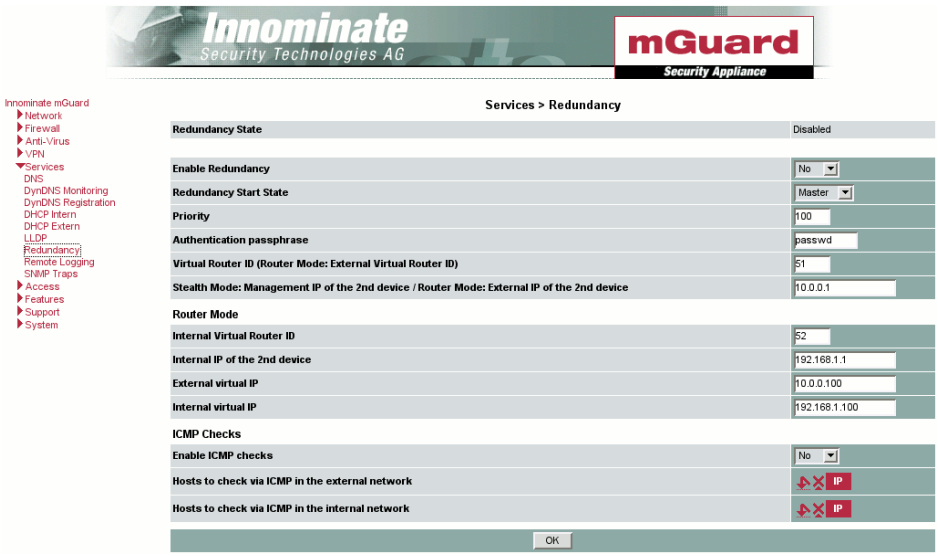
Port description

A textual description of the remote device's interface.

System name

Hostname of the remote device.

Services → Redundancy (mGuard enterprise XL only)



The redundancy feature allows two mGuards to be configured to operate as a virtual router. In case of an error, one mGuard (the *backup*) will take over the functionality of the other mGuard (previously working as the *master*).
Additionally, the state of the statefull firewall is synchronized between both mGuards so that, in case of a switch, current connections will not be interrupted.

- ☒ Prerequisite: Both mGuards must be configured accordingly. The firewall configuration should be identical to avoid problems after a switch.
- ☒ Redundancy can only be used in router mode, static stealth mode with management IP or multi stealth mode.
- ☒ The mGuards operating as virtual router must not be used as a VPN gateway.
- ☒ Devices connected to the internal network of the virtual router configuration must be configured to use the internal virtual IP as the default gateway.

The following features are supported by the virtual router configuration:

- Incoming/Outgoing firewall rules
- NAT (IP-Masquerading, i.e. traffic is NATed to the external virtual IP)
- 1to1 NAT
- Port forwarding (use the external virtual IP as *Incoming on IP*)
- MAC-Filter

Enable Redundancy

Enable/Disable the redundancy feature.

Redundancy Start State

The state of this mGuard during activation of redundancy (master or backup).

Priority

Defines which mGuard will operate as the master.

In case the priorities are different, the mGuard with the higher priority will operate as the master as long as it does not fail.

If both mGuards have the same priority and the backup becomes the master in case of a failure, it will continue to work as the master even when the other mGuard becomes available again.

Values between 1 and 254 are possible.

Authentication passphrase

This password is to protect against missconfiguration among different virtual routers.

The password must be the same on both mGuards. It will be transmitted in clear text and should not be identical with other security relevant passwords.

Virtual Router ID (Routermode: External Virtual Router ID)

An ID between 1 and 255 which must be the same on both mGuards and identifies the virtual router.

Management IP of the 2nd device (Routermode: External IP of the 2nd device)

In stealth mode the management IP of the other mGuard, in router mode the external IP of the other mGuard.

Router Mode

The following values need to be set if the mGuards are operated in router mode.

Internal Virtual Router ID

An ID between 1 and 255 which must be the same on both mGuards and identifies the virtual router on the internal interface.

Internal IP of the 2nd device

The internal IP of the other mGuard.

External virtual IP

IP of the virtual router on the external interface (WAN).

Internal virtual IP

IP of the virtual router on the internal interface (LAN). Clients inside the internal network should use this IP as their default gateway.

ICMP Checks

ICMP checks provide an additional way to monitor the network connections between mGuards working as a virtual router.

The backup will also become the master if only one of the internal or external network connections between master and backup fails. Since the Virtual Router Redundancy Protocol (VRRP) used by the mGuard does not provide a feature to inform the master of this change, both mGuards would now be conflicting masters on the remaining network connection.

With ICMP checks (ICMP ping), the master can check its connections to the bakkup and deactivate itself in case its internal or external connections to the backup failed.

Enable ICMP Checks

The master mGuard will check the connection to the backup mGuard using the ICMP ping protocol.

In case the backup mGuard can not be reached, the *Hosts to check via ICMP in the external/internal network* will be tried. If these checks fail as well, the master mGuard will deactivate itself.

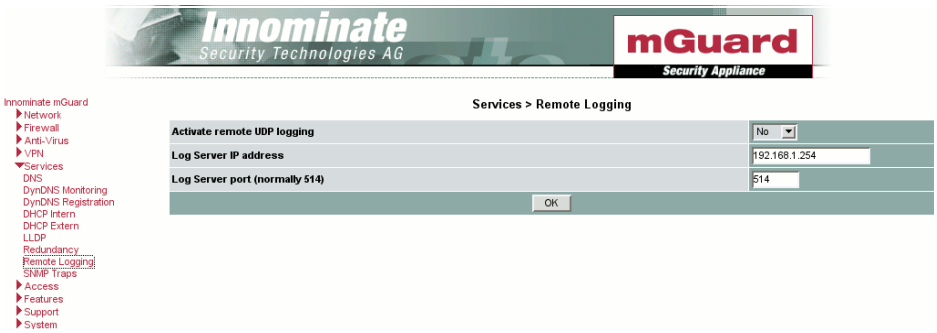
Hosts to check via ICMP in the external network

Hosts in the external network to be checked. The hosts have to be able to answer to the ICMP echo requests.

Hosts to check via ICMP in the internal network

Hosts in the external network to be checked.The hosts have to be able to answer to the ICMP echo requests.

Services → Remote Logging (mGuard enterprise only)



All log entries are recorded in the mGuard's temporary memory (RAM). Once the space for log entries has been filled, the oldest log entries will be overwritten. Furthermore, if the mGuard is switched off, all log entries are deleted.

If you wish to keep a copy of the log, the log entries can be sent to an external system. This is particularly useful if you wish to have centralised administration of the logs.

Activate remote UDP logging Yes / No

If all log entries should be sent to an external (specified below) log server, set this option to **Yes**.

Log Server IP address

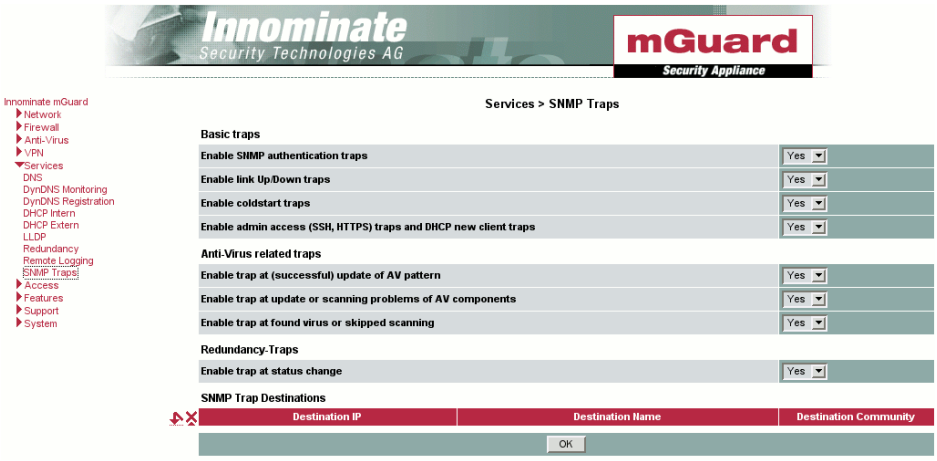
Enter the IP address of the log server to which the log entries should be sent via UDP.

☞ This entry must be an IP address - not a hostname! This function does not support hostnames, since, if it did, it would not be possible to log the loss of a DNS server.

Log Server port

Enter the port of the log server to which the log entries should be sent via UDP. Standard: 514

Services → SNMP Traps (mGuard enterprise only)



The mGuard can send SNMP traps on certain events. The following settings are possible:

Basic traps

- Enable SNMP authentication traps
- Enable link Up/Down traps
- Enable coldstart traps
- Enable admin access (SSH, HTTPS) traps and DHCP new client traps

Anti-Virus related traps

- Enable trap at (successfull) update of AV pattern
- Enable trap at update or scanning problem of AV components
- Enable trap at found virus or skipped scanning

Redundancy-Traps

- Enable trap at status change.

SNMP Trap Destinations

Traps can be send to one or more targets.

Destination IP

IP, to which the trap shall be send.

Destination Name

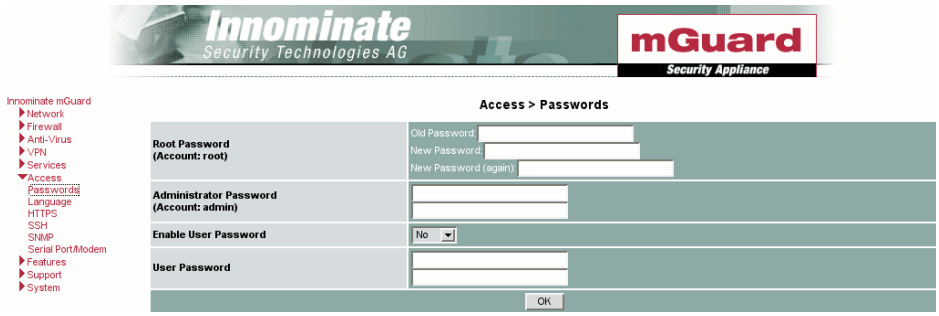
An optional descriptive name for the destination, which has no influence on the generated traps.

Destination Community

Name of the traps SNMP community.

5.11 Access Menu

Access → Passwords



The mGuard supports 3 levels of user authorization. To login at a specific level of authorization, the user must enter the corresponding password for the level.

Authorization level	
Root	This level (password) grants full rights to all parameters of the mGuard. Note: This is the only authorization level that allows you to setup a SSH connection to the device and to then change all of the parameters so that nothing will work any more. If this happens, all you can do is "flash" the firmware to restore it to the factory settings (see "Flashing the firmware" on page 91). Default root password: **root**
Administrator	If you login at this level (password), you will be granted all the rights required for the configuration options that are accessible via the Web-based Administrator interface. Default user name: **admin** Default password: **mGuard** The user name **admin** cannot be changed.
User	If a user password has been defined and activated, the user must – after every restart of the mGuard – enter this password to enable a VPN connection when he or she first attempts to access any HTTP URL. If you wish to use this option, enter the desired user password once in each of the corresponding entry fields.

Root Password

Factory (default) setting: **root**

If you wish to change the root password, enter the current password in the *Old Password* field and then the desired new password in the two corresponding fields below.

Administrator Password (Account: admin)

Factory (default) setting: **mGuard** (fixed user name: admin)

Enable User Password: No / Yes

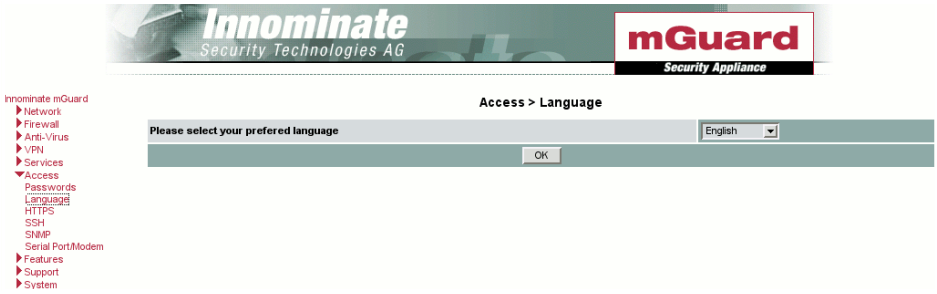
The factory setting for this option is "No".

If a user password is set below, this option can be used to activate/deactivate user password protection.

User Password

There is no factory setting for the user password. To set one, enter the desired password twice - once in each of the two fields.

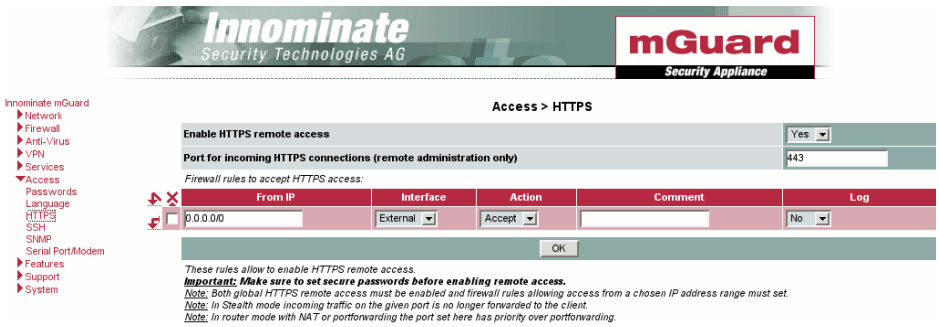
Access → Language



Please select your preferred language

If **(Automatic)** is selected from the list of languages, the device will use the language setting of the system's browser.

Access → HTTPS



When HTTPS Remote Access is enabled, the mGuard can be configured – using its Web-based Administrator interface – from a remote system. In other words, a browser running on the remote system will be used to configure the local mGuard.

This option is disabled by default.

IMPORTANT:If you enable remote access, make certain that you have secure root and administrator passwords.

To enable HTTPS remote access, proceed as follows:

Enable HTTPS remote access: Yes / No

If you want to enable a HTTPS connection, set this switch to **Yes**.

☞ In this case, make certain that the firewall rules on this page permit the mGuard be accessed from a remote site.

Port for incoming HTTPS connections (remote administration only)

Standard: 443

You can select a different port.

If a different port has been selected, you must append the port number (set here) to the IP address of the device in the address provided by the remote site, which will have remote access.

Example:

If this mGuard can be found in the Internet at the address 123.456.789.21 and the Port Number 443 has been set as the port for remote access, you need not enter this port number after the address in the Web browser's address field on the remote system.

If a different Port Number is used, this must be appended to the IP address, e. g as follows.: https://123.456.789.21:442/

Firewall rules to accept HTTPS access

Lists the firewall rules that have been set. These apply for the incoming data packets of an HTTP remote access.

☞ Inserting, moving and deleting rows is explained under "Working with tables" on page 16.

From IP

Enter the address(es) of the system(s) that is/are allowed remote access in this field.

You have the following options for the entries:

- IP address: **0.0.0.0/0** means all addresses. To enter an address space, use the CIDR notation – see "CIDR (Classless InterDomain Routing)" on page 89.

Interface

External (preset – cannot be changed).

Action

Possible settings:

- Accept
- Reject
- Drop

Accept means that the data packets should be passed through.

Reject means that the data packets should be rejected so that the sender is informed that the data packets have been rejected. (In *Stealth* mode, *Reject* has the same effect as *Drop* see below.)

Drop means that the data packets should not be passed through. The data packets will be discarded so that the sender will not be informed as to what happened to them.

☞ In Stealth mode, *Reject* is not supported.

Comment

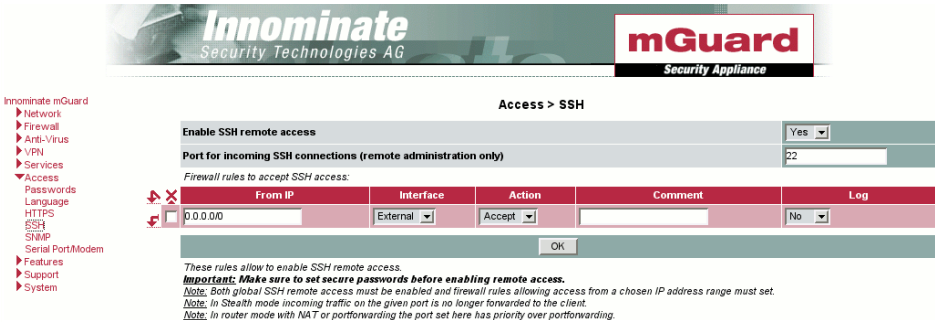
An informational comment for this rule.

Log

You can specify - for each individual firewall rule - whether the use of the rule

- should be logged by setting - *Log* to **Yes**
- or should not be logged by setting - *Log* to **No** (factory setting).

Access → SSH



When SSH Remote Access is enabled the mGuard can be configured from a remote system using the command line interface.
This option is disabled by default.

IMPORTANT:If you enable remote access, make certain that you have secure root and administrator passwords.

To enable SSH Remote Access, proceed as follows:

Enable SSH remote access: Yes / No

If you want to allow SSH connections, set this switch to **Yes**.

☞ In this case, make certain that the firewall rules on this page permit the mGuard be accessed from a remote site.

Port for incoming SSH connections (remote administration only)

Standard: 22

You can select a different port.

Example:

If this mGuard can be found in the Internet at the address 123.456.789.21 and the Port Number 22 has been set as the port for remote access, you may need not enter this port number in the address field on the remote system's SSH client.

If a different port number has been set (e.g. 22222), this must be specified to the SSH client, e.g.:

ssh -p 22222 123.456.789.21

Firewall rules to accept SSH access

Lists the firewall rules that have been set. These apply for the incoming data packets of an SSH remote access.

☞ Inserting, moving and deleting rows is explained under “Working with tables” on page 16.

From IP

Enter the address(es) of the system(s) that is/are allowed remote access in this field.

You have the following options for the entries:

- IP address: **0.0.0.0/0** means all addresses. To enter an address space, use the CIDR notation – see “CIDR (Classless InterDomain Routing)” on page 89.

Interface

External (preset – cannot be changed).

Action

Possible settings:

- Accept
- Reject
- Drop

Accept means that the data packets should be passed through.

Reject means that the data packets should be rejected so that the sender is informed that the data packets have been rejected. (In *Stealth* mode, *Reject* has the same effect as *Drop*.)

Drop means that the data packets should not be passed through. The data packets will be discarded so that the sender will not be informed as to what happened to them.

☞ In Stealth mode, *Reject* is not supported.

Comment

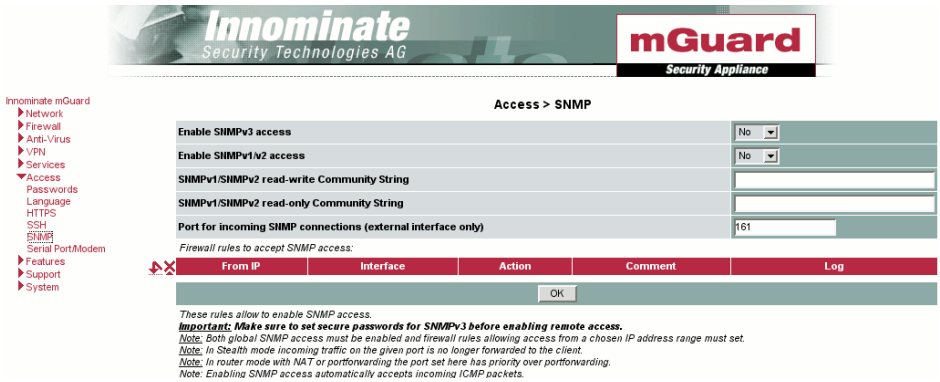
An informational comment for this rule.

Log

You can specify - for each individual firewall rule - whether the use of the rule

- should be logged by setting - *Log* to **Yes**
- or should not be logged by setting - *Log* to **No** (factory setting).

Access → SNMP (mGuard enterprise only)



SNMP (Simple Network Management Protocol) is mainly used in more complex networks to monitor the status and operation of devices.

SNMP is available in several releases: SNMPv1/SNMPv2 and SNMPv3.

The older versions SNMPv1/SNMPv2 do not use encryption and are not considered to be secure. We therefore recommend that you do not use SNMPv1/SNMPv2.

As far as security is concerned, SNMPv3 is considerably better, but not all management consoles support it.

⌧ It can take more than one second to process SNMP- “get” or “walk” requests. However the factory settings for the time-out of many Network Management Applications is set to one second. In case you experience time-out problems, please set the time-out of your Management Application to values between 3 and 5 seconds.

Enable SNMPv3 access: Yes / No

If you wish to allow monitoring of the mGuard via SNMPv3, set this switch to **Yes**.

The access via SNMPv3 requires an authentication with a login and a password. The factory settings for these entries are:

Login: admin

Password: SnmpAdmin

MD5 is supported for the authentication; DES is supported for encryption.

The login parameters for SNMPv3 can be changed only by using SNMPv3.

Enable SNMPv1/v2 access: Yes / No

If you wish to allow monitoring of the mGuard via SNMPv1/v2, set this switch to **Yes**.

In addition, you must enter the following login data:

SNMPv1/SNMPv2 read-write Community String

SNMPv1/SNMPv2 read-only Community String

Enter the required login data in these two fields.

Port for incoming SNMP connections (external interface only)

Standard: 161

Firewall rules to accept SNMP access

Lists the firewall rules that have been set. These apply for the incoming data packets of an SNMP remote access.

☞ Inserting, moving and deleting rows is explained under “Working with tables” on page 16.

From IP

Enter the address(es) of the system(s) that is/are allowed access for the purpose of SNMP monitoring in this field.

You have the following options for the entries:

- From IP
- **0.0.0.0/0** means all addresses. To enter an address space, use the CIDR notation – see “CIDR (Classless InterDomain Routing)” on page 89.

Interface

External (preset – cannot be changed).

Action

Possible settings:

- Accept
- Reject
- Drop

Accept means that the data packets should be passed through.

Reject means that the data packets should be rejected so that the sender is informed that the data packets have been rejected. (In *Stealth* mode, *Reject* has the same effect as *Drop*.)

Drop means that the data packets should not be passed through. The data packets will be discarded so that the sender will not be informed as to what happened to them.

☞ In Stealth mode, *Reject* is not supported.

Comment

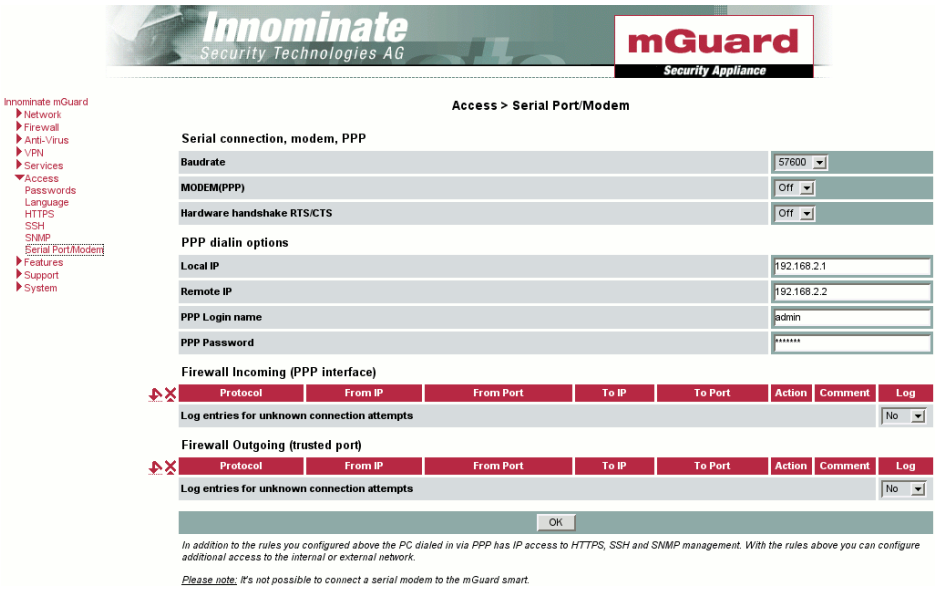
An informational comment for this rule.

Log

You can specify - for each individual firewall rule - whether the use of the rule

- should be logged by setting - *Log* to **Yes**
- or should not be logged by setting - *Log* to **No** (factory setting).

Access → Serial Port/Modem



Some mGuards, like the mGuard blade or industrial, offer a serial interface that can be used to access the mGuard with a terminal client or a PPP connection.

Serial connection, modem, PPP

Baudrate

The speed of the serial port.

MODEM(PPP)

When set to **Off** , the serial interface can be used with a terminal client. When set to **On**, the serial interface can be used with PPP.

Hardware handshake RTS/CTS

Use the RTS and CTS signals for the PPP connection.

PPP dialin options

Local IP

IP of the mGuard for the PPP connection.

Remote IP

IP of the remote peer for the PPP connection.

PPP Login name

Login to be send by the remote PPP peer.

PPP Password

Password to be send by the remote PPP peer.

Firewall Incoming (PPP-Interface)

Firewall rules for connection from the PPP to the internal ethernet interface (LAN).

☞ Inserting, moving and deleting rows is explained under “Working with tables” on page 16.

You have the following options for the entries:

Protocol

All means: TCP, UDP, ICMP and other IP protocols.

IP address

0.0.0.0/0 means all addresses. To enter an address space, use the CIDR notation – see “CIDR (Classless InterDomain Routing)” on page 89.

Port

(This is only evaluated by the TCP and UDP protocols)

any means each and every port.

startport:endport (e.g. 110:120) defines a range of ports.

You can specify individual ports by giving either their port number or the corresponding service name: (e.g. 110 for pop3 or pop3 for 110).

Action

Accept means that the data packets are passed through.

Reject means that the data packets are rejected so that the sender is informed that the data packets have been rejected. (In *Stealth* mode, Reject has the same effect as *Drop* (see below).)

Drop means that the data packets are not passed through. The data packets will be discarded so that the sender will not be informed as to what happened to them.

Comment

An informational comment for this rule.

Log

You can specify - for each individual firewall rule - whether the use of the rule

☞ should be logged by setting - *Log* to **Yes**

☞ or not by setting - *Log* to **No** (factory setting).

Log entries for unknown connection attempts

If this is set to Yes, all attempts to establish a connection, which were not covered by the rules defined above, will be logged.

Firewall Incoming (PPP-Interface)

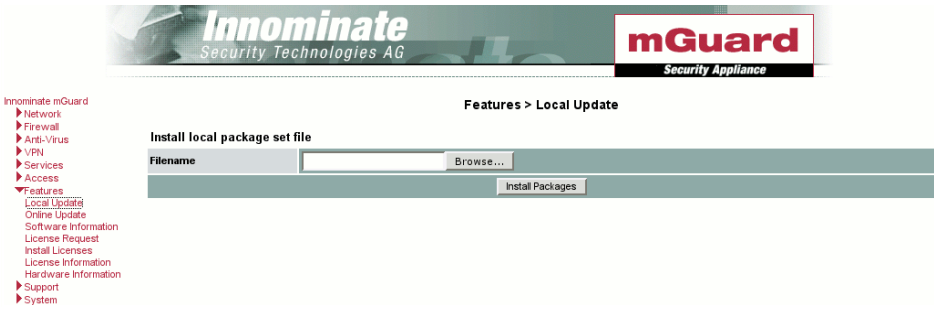
Firewall rules for connection from the the internal ethernet interface (LAN) to PPP.

(All other settings conform to *Firewall Incoming (PPP-Interface)*.)

5.12 Features Menu

Features → Local Update

Please read the README file!



Prerequisite: You must have a current software package saved locally on your configuration system.

⌧ For information as to whether or not and, if so, in which manner you can obtain a software update, please contact your distributor.

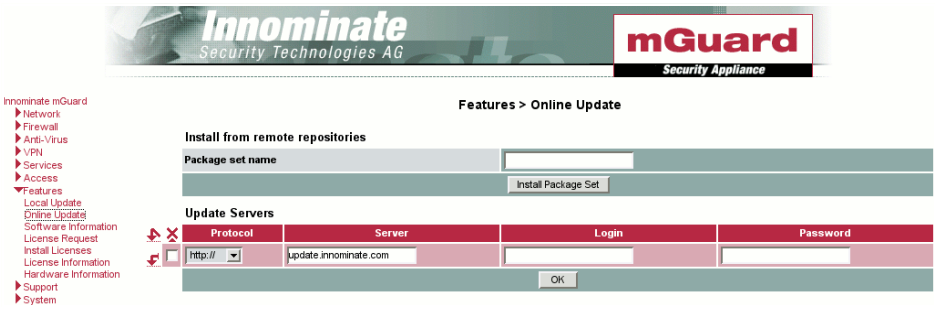
⌧ **Do not interrupt the power supply during the update procedure! Otherwise the device could be damaged and may be left inoperable, and will require your device to be send to the manufacturer.**

Once you have a current software update saved on your configuration system, proceed as follows:

1. Click on **Browse...** and then select the file.
2. Click on **Install Packages** to transfer them to the device.
   Depending on the size of the update, this may take several minutes.

If a reboot is necessary after a system update, a message to this effect will be displayed.

Features → Online Update



Prerequisite: You must have a current software package available from a remote server.

⌧ For information as to whether or not and, if so, in which manner you can obtain a software update, please contact your distributor.

⌧ **Do not interrupt the power supply during the update procedure! Otherwise the device could be damaged and may be left inoperable, and will require your device to be send to the manufacturer.**

Proceed as follows:

1. Enter the update's name in the entry field, e.g. "update-"
2. Click on **Install Package Set** to transfer them to the device.
   Depending on the size of the update, this may take several minutes.

If a reboot is necessary after a system update, a message to this effect will be displayed.

Update Server

Here you can specify the servers from which the mGuard shall retrieve its updates.

Protocol

The update files can be downloaded using either FTP or HTTP.

Server

In this field, enter the FQDN or IP address of the server from which the update files shall be downloaded, eg. “123.456.789.21” or “update.example.com”.

Login

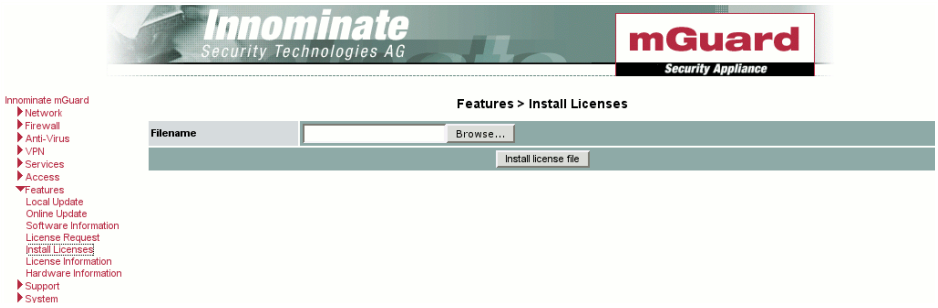
In this field, enter the user name to be used for connecting to the server.

Password

In this field, enter the password to be used when logging in.

☞ Inserting, moving and deleting rows is explained under “Working with tables” on page 16.

Features → Install Licenses

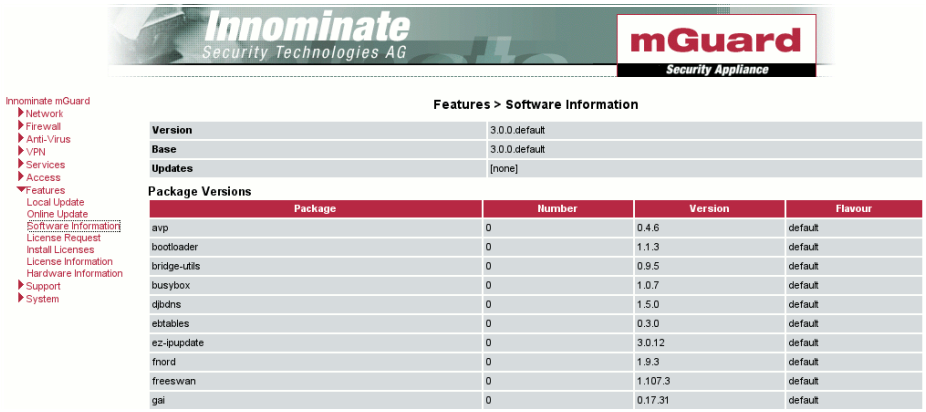


Prerequisite: You must have purchased a license file for the mGuard from your distributor and must have saved this file on the configuration system.

To install the license file, proceed as follows:

1. Click on **Browse...** and then select the file.
2. Click on **Install Licenses** to transfer them to the device.

Features → Software Information



Display only:

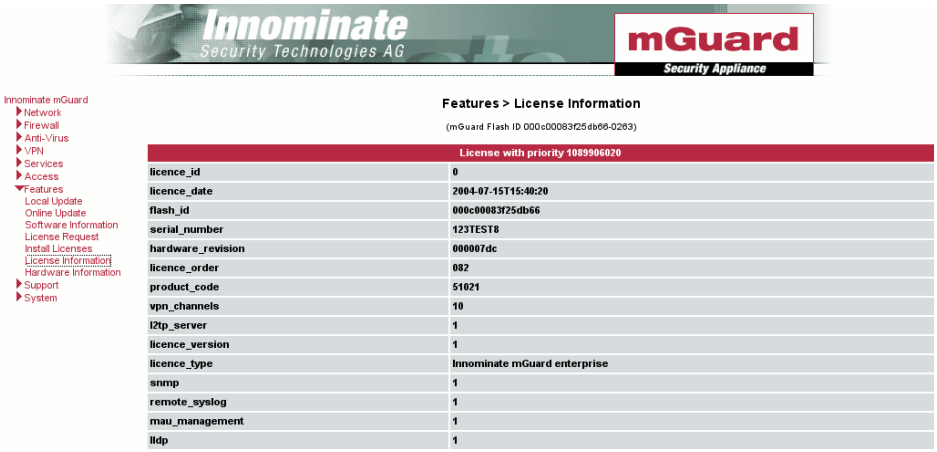
This page lists the software modules (packages) currently loaded in the device. Each of these is called a package.

The purpose of this page is to provide the information required prior to making an update: Compare the displayed package version numbers with those of the

corresponding current packages. For the relevant information. please contact your distributor.
If new versions are available, you can update the software in the device. See “Features ‡ Local Update” on page 79.

Features → License Information

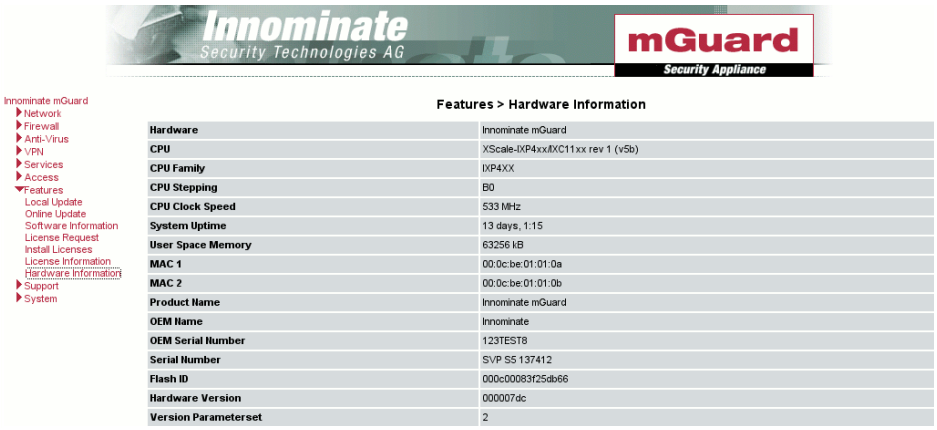
Display only:



Lists the purchased licenses. The corresponding license files are installed on the mGuard. See “Features ‡ Install Licenses” on page 80.

Features → Hardware Information

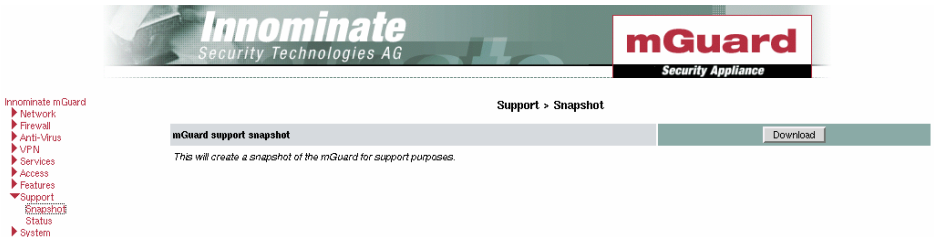
Display only:



Only for experienced system administrators or support.

5.13 Support Menu

Support → Snapshot



This function is intended to provide the support with the necessary diagnostic information.

This function prepares a compressed file (in tar format) containing all of the current configuration settings and log entries, which could be relevant to the diagnosis of errors. (This file does not contain any private information such as the private machine certificate or the passwords.) Any Pre-Shared Keys for VPN connections are, however, included in the snapshot.)

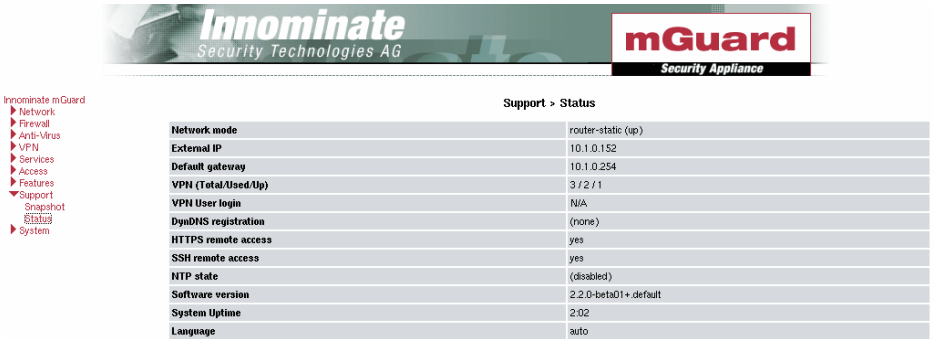
To take a snapshot, proceed as follows:

1. Click on **Download**.
2. Save the file under the name *snapshot.tar.gz*

Please make the file available to the support, if requested.

Support → Status

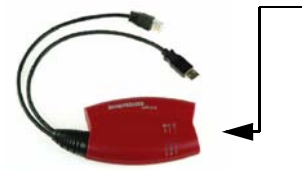
Display only:



This presents a summary of various status information required for the purpose of support:

Network mode: Displays the mGuard's operating mode: *Stealth*, *Router*, *PPPoE* or *PPTP*

External IP: This field shows the mGuard‘s IP address for the network interface used for its external network (WAN or Internet).
In *Stealth* mode, the mGuard takes the address of the locally connected computer for this interface.

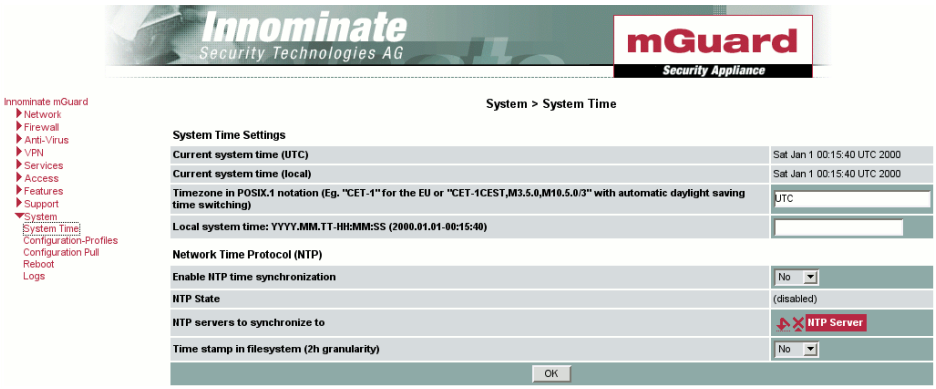


Default gateway: The IP address over which the mGuard will route connections to networks unknown to him.
In *Stealth* mode or in case the configured IP isn’t inside a known network this field will show “(none)”.

VPN (Total / Used / Up):	Possible settings: *Total / Used / Up* *Total*: Total number of VPN connections setup *Used*: Number of VPN connections used *Up*: Number of VPN connections currently active
VPN User login:	Possible settings: *N / A* : (not available) *not logged in*: VPN disabled *logged in*: VPN enabled
DynDNS registration:	Possible settings: *none / DynDNS Server / failure / trying* *none*: No DynDNS server specified. *DynDNS Server*: Address of the DynDNS server, which the mGuard will use to register hostnames. *failure*: The mGuard has unsuccessfully attempted to setup a connection to the DynDNS server. *trying*: The mGuard is attempting to setup a connection to the DynDNS server.
HTTPS remote access:	Possible settings: *no / yes*
SSH remote access:	Possible settings: *no / yes*
NTP state:	Possible settings: *synchonized / not synchronized* *synchronized*: The mGuard obtains the current time (Greenwich Mean Time) from a time server via the Network Time Protocol. *not synchronized*: The mGuard is not connected to a time server and, therefore, cannot supply the current time.
Software version:	Shows the version of the software installed in the mGuard
System Uptime:	This shows how much time has elapsed since the last time that the mGuard was started.
Language:	This field shows the currently selected language.

5.14 System Menu

Services → System Time



System Time Settings

Current system time (UTC)

Displays the current system time in Universal Time Coordinates (UTC). If the *Enable NTP time synchronisation* is not yet activated (see below) and *Time stamp in filesystem* is deactivated, the clock will start with 1 January 2000.

Current system time (local)

If the possibly differing current local time should be displayed, you must make the corresponding entry under *Timezone in POSIX.1 notation...* (see below).

Timezone in POSIX.1 notation...

If the Current *system time* above should display your current local time instead of the current time (if it is different to the Greenwich Mean Time), you must enter the number of hours (plus or minus) that your local time differs from Greenwich Mean Time.

Examples:

In Germany, the time is one hour earlier than in Greenwich. Therefore, enter: CET-1

In the entry, the characters preceding the -1, -2 or +1 etc. are not considered. Only the numerical difference is important. The characters preceding the numerical difference may be “CET” or any other acronym that you find useful.

If you wish to display Central European Time (for example for Germany) and have it automatically switch to/from daylight saving time, enter: CET-1CEST,M3.5.0,M10.5.0/3

Local system time

Here you can set the mGuard’s in case no NTP server has been specified or the NTP server isn’t reachable.

The date and time are specified in the format YYYY.MM.DD-hh:mm:

YYYY	Year
MM	Month
DD	Day
hh	Hour
mm	Minute

Network Time Protocol (NTP)

Enable NTP time synchronisation Yes / No

Once the NTP is enabled, the mGuard takes the time from the Internet and displays this as its current system time. The synchronisation can take several seconds.

If this option is set to **Yes** and at least one time server is specified under *NTP servers to synchronize to* (see below), the current system time will be retrieved over the internet.

NTP State

Displays the current NTP state

NTP servers to synchronize to

Under this option, enter one or more time servers from which the mGuard should obtain the current time. If you enter multiple time servers, the mGuard will automatically connect with all of them to determine the current time.

☞ If you enter a hostname, e.g. pool.ntp.org, instead of an IP address, a DNS server must also be specified - see “Services ‡ DNS” on page 62.

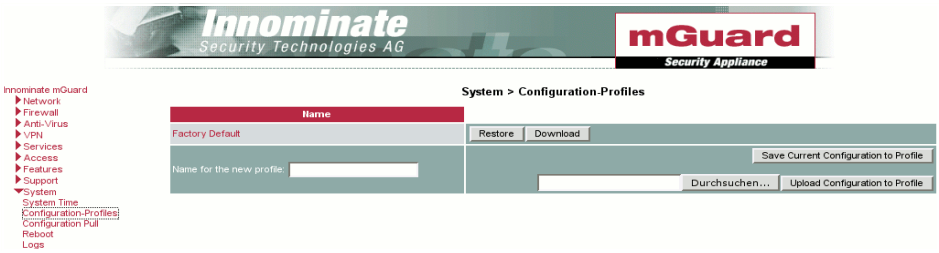
☞ If the mGuard is operating in *Router*, *PPPoE* or *PPTP* mode, it will also make the NTP time available to the locally connected systems.

Time stamp in filesystem (2hr granularity): Yes / No

If this option is set to **Yes**, the mGuard will save the current system time to its memory every two hours.

Afterwards: If the mGuard is switched off and back on, a time from this two hour period of time will be displayed when the mGuard is switched on and not (the factory setting) a time on 1 January 2000.

System → Configuration Profiles



You can save the configuration settings as a configuration profile under any name in the mGuard. You can create and save multiple configuration profiles. You can then select and activate the configuration profile appropriate at the time, if you use the mGuard in different operating environments.

Furthermore, you can also save configuration profiles as files on the configuration system. Naturally, these configuration files can then be read back into the mGuard and activated.

Furthermore, you can restore the mGuard to the factory settings at any time.

⌧ Passwords and user names are not saved in the configuration profiles.

Saving the current configuration in the mGuard as a profile

1. In the *Name for the new profile:* field, enter the desired name
2. Click on the **Save Current Configuration to Profile** button.

Displaying / Activating / Deleting a configuration profile stored in the mGuard

Displaying a configuration profile:

Click on the name of the configuration profile.

Activating a configuration profile:

Click on the **Restore** button at the right of the name of the configuration profile.

⌦ If the restored configuration includes a change between stealth mode and one of the other network modes, the mGuard will be rebooted.

Deleting a configuration profile:

Click on the **Delete** button at the right of the name of the configuration profile. The profile **Factory Default** can not be deleted.

Saving a configuration profile as a file (on the configuration system)

1. Click on the **Download** button at the right of the name of the configuration profile.
2. Enter the filename and folder (where the configuration profile should be saved) in the displayed dialog.
   (You can give the file any name desired.)

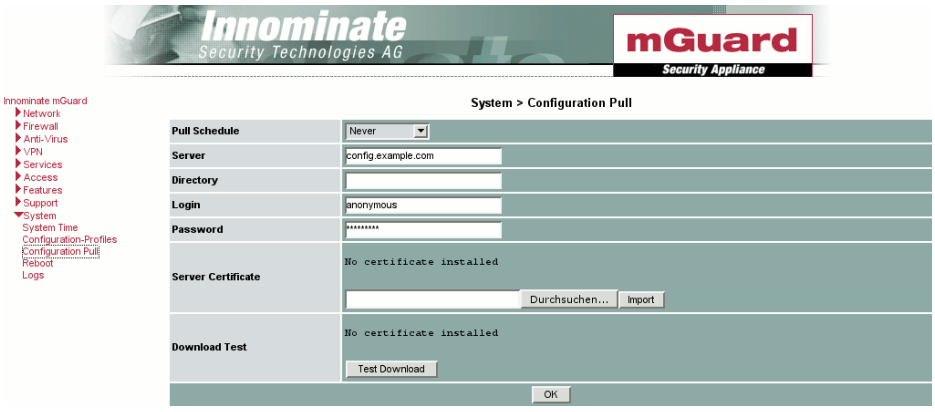
Uploading a configuration profile from a configuration system to the mGuard

Prerequisite: Naturally, you must stored (as described above) at least one configuration profile as a file on the configuration system.

1. In the *Name for the new profile* field, enter the name that should be assigned to configuration profile uploaded from the configuration system.
2. Click on **Choose** and then select the file.
3. Click on the **Upload Configuration to Profile** button.
   Afterwards: The uploaded configuration will now be displayed in the list of configuration profiles.

If you want to activate the uploaded configuration profile, click on the **Restore** button next to the name.

System → Configuration Pull



The mGuard can retrieve new configuration profiles from a HTTPS server in configurable time intervalls. When a new configuration differs from the current configuration, it will be activated automatically.

Pull Schedule

Intervall, at which new configurations will be searched on the server

Server

IP or Hostname of the server, which provides the configuration profiles.

Directory

The directory on the service in which the configuration is located.

Login

The login on the HTTPS server.

Password

The Password on the HTTPS server.

Server Certificate

The certificate, which authenticates the HTTPS server from which the configuration is fetched. It is used to prevent unauthorized configurations from being installed on the mGuard.

☞ The name of the configuration file on the HTTPS server is the mGuards serial number with the suffix ".atv".

☞ In case the configuration profiles do contain the machine certificate or PSKs for VPN connections the password should consist of at least 30 random upper and lower case letters and numbers, in order to prevent unallowed access to the keys.
The HTTPS server should further only grant access to a single configuration profile per login and password. Otherwise users of other or even compromised mGuards may gain access to other configurations.

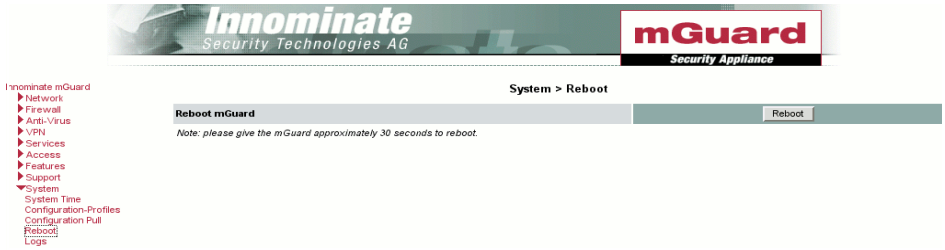
☞ Self signed certificates should not use the “key-usage” extension.

Download Test

Tests the specified parameters without actually saving them or activating the profile. The result of the test will be displayed in the right column.

⌧ You should make sure that the profile on the server doesn’t contain unwanted variables beginning with “GAI_PULL_” which overwrite the pull configuration made here.

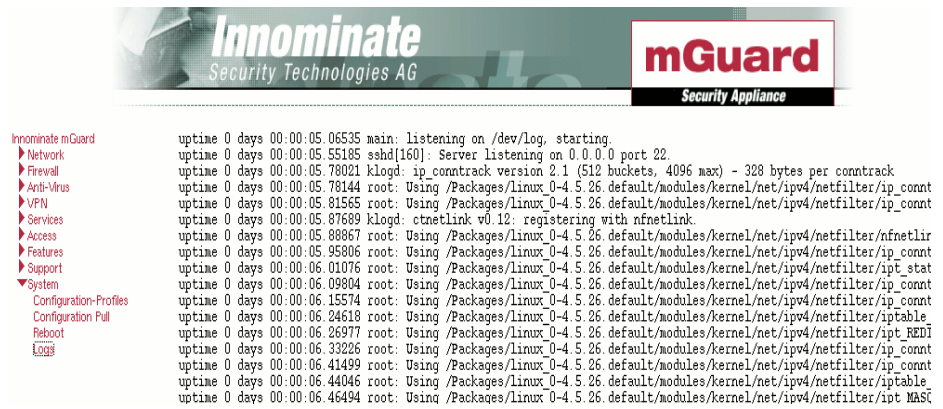
System → Reboot



A new start (= reboot) is necessary in the event that a fault occurs. It may also be necessary after a software update.
Once the mGuard has completed the restart, a message is displayed that you can continue the configuration.
You can also reboot the device by switching it off and back on again.

System → Logs

Display only:


Innominate Security Technologies AG
mGuard
Security Appliance
Innominate mGuard
Network
Firewall
Anti-Virus
VPN
Services
Access
Features
Support
System
Configuration-Profiles
Configuration Pull
Reboot
Logs
uptime 0 days 00:00:05.06535 main: listening on /dev/log, starting.
uptime 0 days 00:00:05.55185 sshd[160]: Server listening on 0.0.0.0 port 22.
uptime 0 days 00:00:05.78021 klogd: ip_conntrack version 2.1 (512 buckets, 4096 max) - 328 bytes per conntrack
uptime 0 days 00:00:05.78144 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/ip_conntr
uptime 0 days 00:00:05.81565 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/ip_conntr
uptime 0 days 00:00:05.87689 klogd: ctnetlink v0.12: registering with nfnetlink.
uptime 0 days 00:00:05.88867 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/nfnetlir
uptime 0 days 00:00:05.95806 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/ip_conntr
uptime 0 days 00:00:06.01076 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/ipt_stat
uptime 0 days 00:00:06.09804 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/ip_conntr
uptime 0 days 00:00:06.15574 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/ip_conntr
uptime 0 days 00:00:06.24618 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/iptable_
uptime 0 days 00:00:06.26977 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/ipt_REDI
uptime 0 days 00:00:06.33226 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/ip_conntr
uptime 0 days 00:00:06.41499 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/ip_conntr
uptime 0 days 00:00:06.44046 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/iptable_
uptime 0 days 00:00:06.46494 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/ipt_MASQ

Shows all of the logged entries (complete log).
The format of the log corresponds to that common under Linux.

Special analysis programs are available which can be used to present the information from the log in a more readable format.
You can send the log entries to an external server. See “” on page 69.

5.15 CIDR (Classless InterDomain Routing)

IP netmasks and CIDR are notations, which define an address space containing multiple IP addresses. In this case, an address space in which the addresses follow one another sequentially is treated as a network.

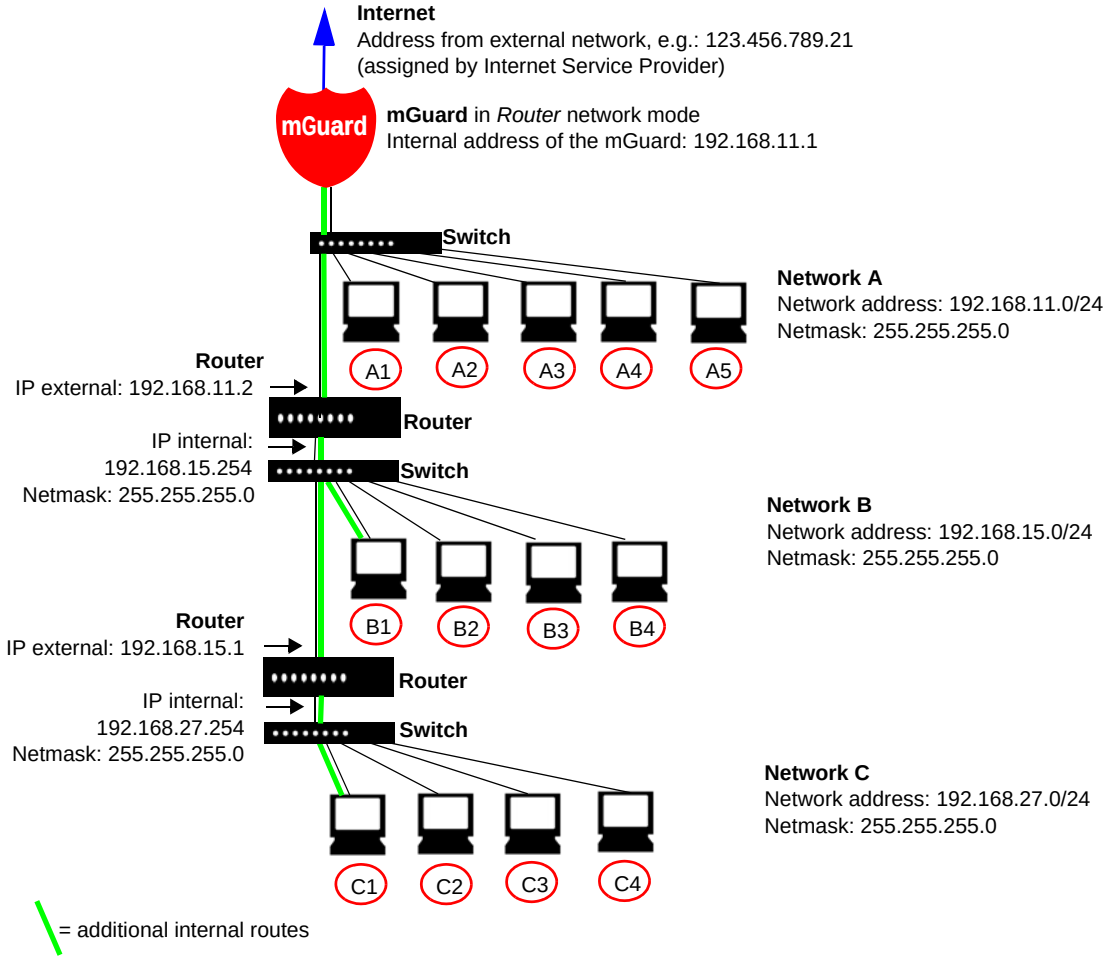
To define a range of IP addresses for the mGuard e.g. when configuring the firewall, it may be necessary to use the CIDR notation to specify the address space. The following table presents the IP netmask on the left and the corresponding CIDR notation on the right.

IP-Netmask	binary				CIDR
255.255.255.255	11111111	11111111	11111111	11111111	32
255.255.255.254	11111111	11111111	11111111	11111110	31
255.255.255.252	11111111	11111111	11111111	11111100	30
255.255.255.248	11111111	11111111	11111111	11111000	29
255.255.255.240	11111111	11111111	11111111	11110000	28
255.255.255.224	11111111	11111111	11111111	11100000	27
255.255.255.192	11111111	11111111	11111111	11000000	26
255.255.255.128	11111111	11111111	11111111	10000000	25
255.255.255.0	11111111	11111111	11111111	00000000	24
255.255.254.0	11111111	11111111	11111110	00000000	23
255.255.252.0	11111111	11111111	11111100	00000000	22
255.255.248.0	11111111	11111111	11111000	00000000	21
255.255.240.0	11111111	11111111	11110000	00000000	20
255.255.224.0	11111111	11111111	11100000	00000000	19
255.255.192.0	11111111	11111111	11000000	00000000	18
255.255.128.0	11111111	11111111	10000000	00000000	17
255.255.0.0	11111111	11111111	00000000	00000000	16
255.254.0.0	11111111	11111110	00000000	00000000	15
255.252.0.0	11111111	11111100	00000000	00000000	14
255.248.0.0	11111111	11111000	00000000	00000000	13
255.240.0.0	11111111	11110000	00000000	00000000	12
255.224.0.0	11111111	11100000	00000000	00000000	11
255.192.0.0	11111111	11000000	00000000	00000000	10
255.128.0.0	11111111	10000000	00000000	00000000	9
255.0.0.0	11111111	00000000	00000000	00000000	8
254.0.0.0	11111110	00000000	00000000	00000000	7
252.0.0.0	11111100	00000000	00000000	00000000	6
248.0.0.0	11111000	00000000	00000000	00000000	5
240.0.0.0	11110000	00000000	00000000	00000000	4
224.0.0.0	11100000	00000000	00000000	00000000	3
192.0.0.0	11000000	00000000	00000000	00000000	2
128.0.0.0	10000000	00000000	00000000	00000000	1
0.0.0.0	00000000	00000000	00000000	00000000	0

Example: 192.168.1.0 / 255.255.255.0 corresponds to 192.168.1.0/24 in CIDR notation

5.16 Network Sketch

The following sketch illustrates, how the IP addresses can be distributed in a local network with subnets, which network addresses result and how the details regarding additional internal routes might look.



Network A

System	A1	A2	A3	A4	A5
IP address	192.168.11.3	192.168.11.4	192.168.11.5	192.168.11.6	192.168.11.7
Netmask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Network B

System	B1	B2	B3	B4
IP address	192.168.15.2	192.168.15.3	192.168.15.4	192.168.15.5
Netmask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Network C

System	C1	C2	C3	C4
IP address	192.168.27.1	192.168.27.2	192.168.27.3	192.168.27.4
Netmask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Additional internal routes

Network:
192.168.15.0/24
Gateway
192.168.11.2

Network:
192.168.27.0/24
Gateway
192.168.11.2

6 The Rescue Button – restart, recovery procedure and to flash the firmware

The Rescue Button is used to set the device in one of the following states:

6.1 Performing a Restart

Objectives To restart the device using the configured settings.

Action: Press the **Rescue Button** for ca. 1.5 seconds, e.g. with a straightened paperclip, until LED 2 is red
ORDisconnect the power briefly.

6.2 Performing a Recovery

Objectives This is used to reset the mGuard to the **Stealth** network mode (mode of operation) so that it can again be accessed (for the purpose of configuring it) at the following address: **https://1.1.1.1/**

⌧ The passwords and the settings configured for VPN connections and the firewall are retained.

Possible reasons for starting the Recovery procedure:
The mGuard is in Router or PPPoE mode and
– the mGuard's IP address has been changed from the default setting and
– you don't know the device's current IP address.

Action:
1. Press the **Rescue Button** slowly 6 times.
2. After about 2 seconds, the mGuard will respond:
   - On success the middle LED lights green
   - On failure the middle LED lights red
3. On success the device will perform a restart and switch to *Stealth* mode. It can then once again be accessed at the following address:
   https://1.1.1.1/

6.3 Flashing the firmware

Objectives To reload the mGuard's complete firmware.

⌧ **All of the configured settings will be deleted.** The mGuard will be restored to the factory (default) settings.

Possible reasons for flashing the firmware:
- The Administrator and Root password have been lost.

Action: Proceed as follows:

⌧ **Do not interrupt the power supply during the flashing procedure.**

Otherwise the device could be damaged and may be left inoperable, and will require your device to be send to the manufacturer.

Prerequisites:

- First copy the mGuard software from the mGuard CD-ROM or retrieve it from Innominate Support and save it on the configuration system.
- A DHCP and a TFTP server, both installed on a single system, which provide the mGuard image files – see “Required before the firmware can be flashed: DHCP and TFTP servers” on page 92.

1. Hold the **Rescue Button** pressed for about 3 seconds and release it when all LEDs become green.
   (If you do not release the **Rescue Button** quickly enough, the mGuard restart again.)
2. The middle LED will flash (heartbeat) and the mGuard tries to receive an IP address from an DHCP server.
3. The 3 green LEDs form a bouncing ball display in which the light shifts from one LED to the next.The file install.p7s will be loaded from the TFTP server, erase the flash memory and load the jffs2.img.p7s file from the TFTP server. This process will take about 3 to 5 minutes.
   The rescue system will only install files digitally signed by Innominate.
4. The middle LED (Heartbeat) will light continuously.
   The new software will be unpacked and configured. This process will take about 5 minutes.
5. As soon as the procedure has been completed, all 3 LEDs will flash green continuously.
6. Restart the mGuard.
   To do so, press the **Rescue Button** briefly.
   OR
   Briefly disconnect and reconnect the USB cable (which is only used to supply power).

The mGuard will be now restored to its factory settings. Configure it once again – see “Setting Up a Local Configuration Connection” on page 14.

Required before the firmware can be flashed: DHCP and TFTP servers

Before the firmware can be “flashed” DHCP and TFTP servers must be installed on the locally connected system or a network system.
(DHCP = **D**ynamic **H**ost **C**onfiguration **P**rotocol; TFTP = **T**rivial **F**ile **T**ransfer **P**rotocol)

Install the DHCP and TFTP server, if necessary (see below).

⌧ If you install a second DHCP server in a network, this can affect the configuration of the entire network!

6.3.1 Installing DHCP and TFTP servers under Windows or Linux

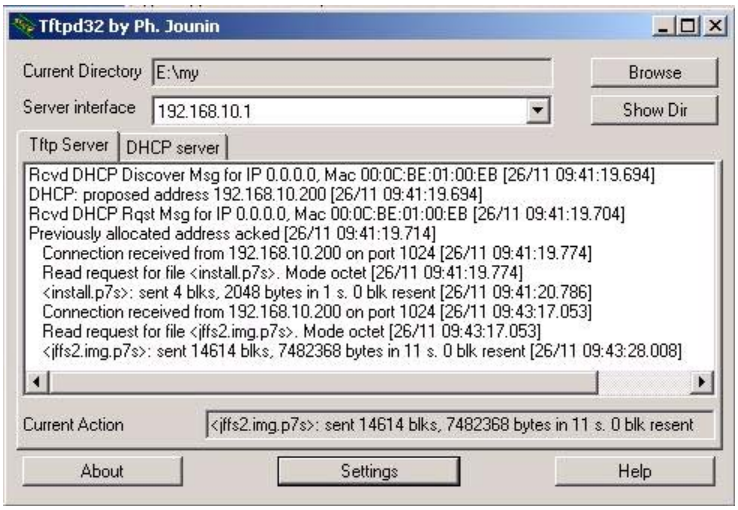
Under Windows:

Install the program found on the CD-ROM. To accomplish this, proceed as follows:

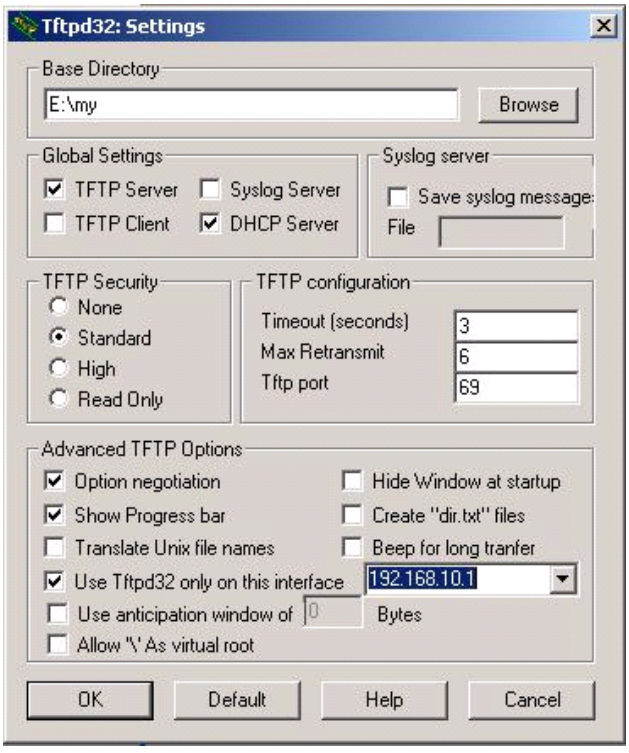
1. If the Windows system is connected to a network, disconnect it.
2. Copy the software into any empty folder on the Windows system. Start the program TFTPD32.EXE
3. The system's IP must be set to: **192.168.10.1.** This must also be the address of the network adapter.

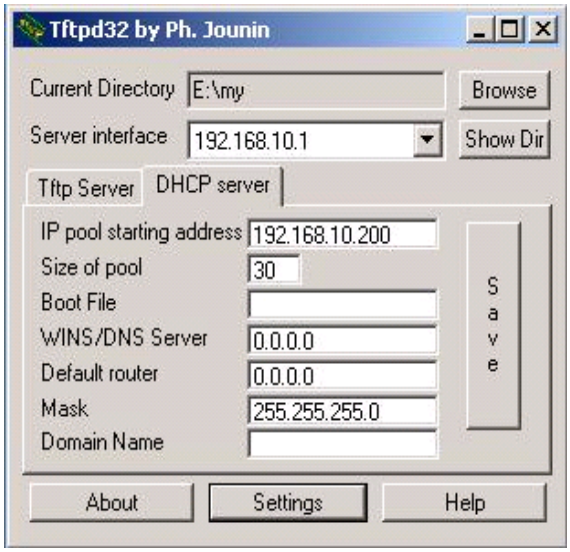
   Click on the **Browse** button to switch to the folder in which the mGuard image files have been saved: *install.p7s, jffs2.img.p7s*

The image files are also found on the CD-ROM, which was included in the package.


Tftpd32 by Ph. Jounin
Current Directory E:\my
Browse
Server interface 192.168.10.1
Show Dir
Tftp Server
DHCP server
Rcvd DHCP Discover Msg for IP 0.0.0.0, Mac 00:0C:BE:01:00:EB [26/11 09:41:19.694]
DHCP: proposed address 192.168.10.200 [26/11 09:41:19.694]
Rcvd DHCP Rqst Msg for IP 0.0.0.0, Mac 00:0C:BE:01:00:EB [26/11 09:41:19.704]
Previously allocated address acked [26/11 09:41:19.714]
Connection received from 192.168.10.200 on port 1024 [26/11 09:41:19.774]
Read request for file <install.p7s>. Mode octet [26/11 09:41:19.774]
<install.p7s>: sent 4 blks, 2048 bytes in 1 s. 0 blk resent [26/11 09:41:20.786]
Connection received from 192.168.10.200 on port 1024 [26/11 09:43:17.053]
Read request for file <jffs2.img.p7s>. Mode octet [26/11 09:43:17.053]
<jffs2.img.p7s>: sent 14614 blks, 7482368 bytes in 11 s. 0 blk resent [26/11 09:43:28.008]
Current Action
<jffs2.img.p7s>: sent 14614 blks, 7482368 bytes in 11 s. 0 blk resent
About
Settings
Help

4. Click on the TFTP Server or DHCP Server tab and then click on the Settings button to open the dialog shown below. Then set the parameters as shown:





Under Linux

All current Linux distributions include DHCP and TFTP servers. Install the corresponding packages as described in the instructions for the respective distribution.
Configure the DHCP server by making the following settings in the **/etc/dhcp file**:

```
subnet 192.168.134.0 netmask 255.255.255.0 {
range 192.168.134.100 192.168.134.119;
option routers 192.168.134.1;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.134.255;}
```

This sample configuration makes 20 IP addresses (.100 to .119) available. It is assumed that the DHCP server has the address 192.168.134.1 (settings for ISC DHCP 2.0).

The required TFTP server is configured in the following file:
/etc/inetd.conf
In this file, insert the appropriate lines or set the necessary parameter for the TFTP service. (The directory for the data is: **/tftpboot)**

```
tftp dgram udp wait root /usr/sbin/in.tftpd -s /tftpboot/
```

Then restart the inetd process to activate the modified configuration.
If you use a different mechanism, e.g. xinetd, please read the corresponding documentation.

7 Glossary

Asymmetrical encryption

In the case of asymmetrical encryption, data is encrypted with one key and decrypted with a second key. Either key may be used for encryption or decryption. One of the keys is kept secret by its owner (Private Key), the other is made available to the public (Public Key), i.e. possible communication partners.
A message encrypted with the public key can only be decrypted and read by the owener of the associated private key. A message encrypted with the private key can only be decrypted and read by a receiver who has the associated public key. The fact that the message was encrypted with the private key proves that the owner of the associated public key actually sent the message. Therefore, the expression "digital signature" is also often used.
However, asymmetrical encryption techniques such as RSA are both slow and susceptible to certain types of attack and are therefore frequently combined with some form of symmetrical encryption (→ symmetrical encryption). On the other hand, there are concepts which avoid the additional work of administering symmetrical keys.

DES / 3DES

This symmetrical encryption algorithm was developed by IBM and checked by the NSA. DES (→ symmetrical encryption) was set in 1977 by the American National Bureau of Standards, which was the predecessor of the National Institute of Standards and Technology (NIST), as the standard for American governmental institutions. Since this was the very first standardized encryption algorithm, it quickly won acceptance by industry even outside of America.
DES uses a 56 bit long key, which is no longer considered secure as the processing power available has greatly increased since 1977.
3DES is a variant of DES. It uses keys that are three times as long, i.e. 168 bits long. 3DES is still considered to be secure and is also included in the IPsec standard.

AES

Advanced Encryption Standard. This encryption standard was developed by NIST (National Institute of Standards and Technology) in cooperation with the industry. This → symmetrical encryption standard was developed to replace the earlier DES standard. AES specifies three different key sizes (128, 192 and 256 bits).
In 1997, NIST started the AES initiative and announced its conditions for the algorithm. From the many proposed encryption algorithms, NIST selected a total of five algorithms for closer examination – the MARS, RC6, Rijndael, Serpent and Twofish algorithms. In October 2000, the Rijndael algorithm was adopted as the standard‘s encryption algorithm.

Client / Server

In a client-server environment, a server is a program or computer, which accepts and answers queries from client programs or computers.
In data communication, a computer which establishes a connection to a server (or host) is also called a client. In other words, the client is the calling computer and the server (or host) is the computer called.

Datagram

In the IP protocol, data is sent in the form of data packets, which are known as IP datagrams. An IP datagram has the following structure:

IP Header	TCP, UDP, ESP etc. Header	Data (Payload)

The IP header contains:

– the IP address of the sender (source IP address)
– the IP address of the receiver (destination IP address)
– the protocol number of the protocol of the next higher protocol layer (in accord with OSI [seven layer] model)
– the IP header checksum used to check the integrity of the received header.

The TCP/UDP header contains the following information:
– the sender's port (source port)
– the recipient's port (destination port)
– a checksum covering the header and some information from the IP header (among others the source and destination IP addresses)

DynDNS provider

Also *Dynamic DNS provider*. Every computer, which is connected to the Internet, has an IP address (IP = Internet Protocol). An IP address consists of a maximum of 4 three-digit numbers, which are each separated by a dot. If the computer accesses its Internet Service Provider (ISP) via a modem on a phoneline, ISDN or ADSL, its ISP will assign it a dynamic IP address. In other words, it will be assigned a different address for every online session. If the computer is online 24 hours a day without interruption (e.g. in the case of a flat rate access), the IP address will even change during the session.
If a local computer should be accessible via the Internet, it must have an address that is known to the remote system. Unless this is true no connection can be established between the remote system and the local computer. If the local computer‘s address is constantly changing, no connection can be setup. Unless, of course, the operator of the local computer has an account with a Dynamic DNS provider (DNS = Domain Name Server).
In this case, the operator can set a host name with this provider under which the system should be reachable, e.g.: www.example.com. The Dynamic DNS provider also supplies a small program, which must be installed and run on this local computer. At each new Internet session, this tool will inform the Dynamic DNS provider which IP address the local computer has currently been assigned. This Domain Name Server will register the current assignment of Domain Name - IP Address and will also inform the other Domain Name Servers in the Internet.
Now, if a remote system wishes to establish a connection to a local system, which is registered with the DynamicDNS provider, the remote system can use the host name of the local system as its address. This will setup a connection to the responsible DNS (Domain Name Server) to lookup the IP address that is currently registered for this hostname. The corresponding IP address will be sent back from the DNS to the remote system, which can then use this as the destination address. The remote system can now directly address the desired local computer.
In principle, all Internet addresses are based on this procedure: First, a connection will be established to a DNS to lookup the IP address assigned for the domain name. Once that has been accomplished, this “looked up” IP address will be used to setup a connection to the desired remote site, which could be any site in the Internet.

IP address

Every host or router in the Internet or an Intranet has a unambiguous IP address (IP = Internet Protocol). The IP address is 32 bits (= 4 bytes) long and is written as 4 three-digit numbers (each in the range from 0 to 255), which are separated by a dot.

An IP address consists of 2 parts: the network address and the host address.

Network Address	Host Address

Each host [or workstation] in a network has the same network address, but a different host address. Depending on the size of the respective network – networks are categorized as Class A, B or C networks, which are each different in size – the two parts of the address differ in length:

	1. Byte	2. Byte	3. Byte	4. Byte
Class A	Network Address	Host Address		
Class B	Network Address		Host Address	
Class C	Network Address			Host Address

Whether the IP address of device in a network is Class A, B or C can be seen in the first byte of the IP address. The following has be specified:

	Value of the 1st Byte	No. of bytes for the network address	No. of bytes for the host address
Class A	1 - 126	1	3
Class B	128 - 191	2	2
Class C	192 - 223	3	1

As you can see, there can be a worldwide total of 126 Class A networks and each of these networks can have a maximum of 256 x 256 x 256 hosts (3 bytes of address space). There can be 64 x 256 Class B networks and each of these networks can have up to 65,536 hosts (2 bytes address space: 256 x 256). There can be 32 x 256 x 256 Class C networks and each of these networks can have up to 256 hosts (1 bytes address space).

Subnet Mask

Normally, a company's network - with access to the Internet - is only officially assigned a single IP address, e.g. 123.456.789.21. Based on the first byte of this sample address, one can see that this company network is a Class B network and therefore the last 2 bytes are free to be used for host addresses. With a Class B network, the company network has address space for up to 65,536 hosts (256 x 256).

Obviously, such huge network is not practical. At this point, one can see a need for subnetworks. The standard answers this need with the Subnet Mask. Like an IP address, this mask is 4 bytes long. The bytes, which represent the network address, are each assigned the value 255. The main purpose of the mask is to "borrow" a portion of the host address which can then be used to address the subnetworks. As an example, by using the subnet mask 255.255.255.0 in a Class B network (2 bytes for the network address, 2 bytes for the host address), the third byte, which was actually intended for host addressing, can now be used for subnet addressing. With this configuration, the company's network could support 256 subnetworks that each have 256 hosts.

IPsec

IP Security (IPsec) is a standard, which uses encryption to verify the authenticity of the sender and to ensure the confidentiality and integrity of the data in IP datagrams (→ Datagram). The components of IPsec are the Authentication Header (AH), the Encapsulating Security Payload (ESP), the Security Association (SA) and the Internet Key Exchange (IKE).
At the start of the session, systems which wish to communicate must determine which technique shall be used and the implications of this choice for the session e.g. *Transport Mode* or *Tunnel Mode*
In *Transport Mode*, an IPsec header will be inserted between the IP header and the TCP or UDP header respectively in each IP datagram. Since the IP header remains unchanged, this mode is only suitable for a host- to-host connection.
In *Tunnel Mode*, an IPsec header and a new IP header will be added in front of the entire IP datagram. As a consequence, the original datagram will be encrypted in its entirety and sent as the payload of the new datagram.
The *Tunnel Mode* is used in VPN applications: The devices at the tunnel ends ensure that the datagrams are encrypted before they pass through the tunnel so the actual datagrams are completely protected while being transferred over the public network.

NAT (Network Address Translation)

Using Network Address Translation (NAT) – which is also often called *IP-Masquerading* – an entire network is "hidden" behind a single device, which is know as a NAT router. The internal computers in the local network with their IP addresses will remain hidden, if you communicate with the outside via a NAT router. The remote system will only see the NAT router with its own IP address.
If the internal computers are to directly communicate with external systems (in the Internet), the NAT router must modify the IP datagrams that are passed back-and-forth between the internal computers and the remote sites.
If an IP datagram is sent from the internal network to a remote site, the NAT router will modify the UDP and TCP headers respectively of the outgoing datagrams. It replaces the source IP address and port with its own IP address and - thus far unused - port. It maintains a table in which the original values are listed together with the corresponding new ones.
When a reply datagram is received, the NAT router will recognize that it is actually for an internal computer from the datagram's destination port. Using the table, the NAT router will replace the destination IP address and port and pass the datagram on via the internal network.

Port Number

The UDP and TCP protocols assign a port number to each peer participating in the connection. This way it becomes possible to handle more than one UDP or TCP connection between two peers at the same time.
Fixed port numbers are assigned for certain, frequently used application processes. These are called a "Assigned Numbers". E.g. HTTP connections are usually established to TCP port 80 or POP3 connections to port 110.

PPPoE

The acronym for **P**oint-to-**P**oint **P**rotocol **o**ver **E**thernet. This protocol is based on the PPP and Ethernet standards. PPPoE defines how to connect users via Ethernet with the Internet via a jointly used broadband medium such as DSL, a Wireless LAN or a cable modem.

PPTP

The acronym for **P**oint-to-**P**oint **T**unneling **P**rotocol. This protocol was developed in a cooperation between Microsoft, U.S. Robotics and others to securely transfer data between VPN nodes (→ VPN) via a public network.

X.509 Certificate

A type of "Seal", which certifies the authenticity of a public key (→

asymmetrical encryption) and the associated data.
To enable the user of the public key, which will be used to encrypt the data, to be sure that the public key that he/she has received is really from its issuer and thus from the instance, which should later receive the data, it is possible to use certification. A *Certification Authority – CA* certifies the authenticity of the public key and the associated link between the identity of the issuer and his/her key. The certification authority will verify authenticity in accordance with its rules, which may, for example, require that the issuer of the public key appear before it in person. Once authenticity has be successfully certified, the certification authority will add its digital signature to the issuer's public key. The result is a Certificate.
An X.509(v3) Certificate thus includes a public key, information about the key owner (given as it Distinguished Name (DN)), the authorized usage etc. and the signature of the certification authority.
The signature is created as follows: The certification authority creates an individual bit sequence, which is known as the HASH value, from the bit sequence of the public key, the information about its owner and other data. This sequence may be up to 160 bits long. The certification authority encrypts this with its own private key and then adds it to the certificate. The encryption with the certification authority's private key proves the authenticity of the certificate, i.e. the encrypted HASH string is the certification authority's digital signature. If the certificate's data is altered, this HASH value will no longer be correct with the consequence that the certificate will be worthless.
The HASH value is also known as the fingerprint. Since it is encrypted with the certification authority's private key, anyone who has the public key can decrypt the bit sequence and thus verify the authenticity of this fingerprint or signature.
The usage of a certification authority means it is not necessary for each owner of a key to know every other owner. It is enough for them to know the certification authority. The additional information about the key further simplifies the administration of the key.
X.509 certificates are used, e.g. for e-mail encryption, in S/MIME or IPsec.

Protocol, communication protocol

Devices, which communicate with each other, must follow the same rules. They must "speak the same language". Such rules and standards are called protocols or communication protocols. Some of the more frequently used protocols include, for example, IP, TCP, PPP, HTTP and SMTP.

Service Provider

Service providers are companies or institutions, which offer users access to the Internet or an online service.

Spoofing, Antispoofing

In Internet terminology, spoofing means supplying a false address. With the false Internet address, the user can create the illusion of being an authorized user.
Anti-Spoofing is term for mechanisms, which detect or prevent spoofing.

Symmetrical encryption

In the case of symmetrical encryption, the same key is used to encrypt and decrypt the data. Two examples of symmetrical encryption algorithms are DES and AES. They are fast, but as the number of users increases the administration becomes rather involved.

TCP/IP (Transmission Control Protocol/ Internet Protocol)

This is a family of network protocols. It is used to connect two computers in the Internet.
IP is the base protocol.
UDP is based on IP and sends individual packets. The packets may arrive at the

recipient in an order different from that in which they were sent or they may even be lost.
TCP secures the connection and ensures, for example, that data packets are passed on the application in the right order.
UDP and TCP add the Port Numbers 1 to 65535 to the IP Addresses. The various services offered by the protocols may be distinguished by these Port Numbers.
A number of additional protocols are based on UDP and TCP, e.g. HTTP (HyperText Transfer Protocol), HTTPS (Secure HyperText Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol, Version 3) and DNS (Domain Name Service).
ICMP is based on IP and adds control messages.
SMTP is an e-mail protocol that is based on TCP.
IKE is an IPsec protocol that is based on UDP.
ESP is an IPsec protocol that is based on IP.
On a Windows PC, the WINSOCK.DLL (or WSOCK32.DLL) handles both protocols.
(→ Datagram)

VLAN

A VLAN (Virtual Local Area Network) divides a physical network into several independent logical networks.
Devices within a VLAN can only access devices within their own VLAN. The membership to a LAN is defined by the physiacl network topology and the VLAN ID (1-4094).

All devices with the same VLAN ID belong to the same VLAN and can therefore communicate with each other.

For a VLAN (based on IEEE 802.1Q) the ethernet frame is extended by 4 bytes, with 12 bits containing the VLAN ID. The VLAN IDs “0” and “4095” are reserved and can’t be used for VLAN identification.

VPN (Virtual Private Network)

A **V**irtual **P**rivate **N**etwork (VPN) connects several separate private networks (subnets) together via a public network, e.g. the Internet, to form a single joint network. A cryptographic protocol is used to ensure confidentiality and authenticity. A VPN thus offers an economical alternative to using dedicated lines to build a nationwide corporate network.

8 Technical data

CPU	Intel IXP 42x, 266 MHz (or 533 MHz, mGuard smart enterprise XL)
Memory	16 MB Flash, 32 MB SDRAM (or 64 MB SDRAM, mGuard smart enterprise XL)
LAN and WAN Interfaces	Ethernet IEEE 802 10/100 Mbps RJ45
Power Supply	From the USB interface (5 V, 500 mA) or an external power supply (110 - 230 V)
Operating System	Innominate Embedded Linux
Monitoring / Indicators	Watchdog and LEDs
Relative humidity	max. 90% (non condensing)
Temperature	0° to 40°C

Notes on CE identification

The devices comply with the regulations of the following European directive: 89/336/EEC Council Directive on the harmonization of the legal regulations of member states on electromagnetic compatibility (amended by Directives 91/263/EEC, 92/31/EEC and 93/68/EEC).

The EU declaration of conformity is kept available for the responsible authorities in accordance with the above-mentioned EU directives at:

Innominate Security Technologies AG
Albert-Einstein-Str. 14
D-12489 Berlin
Telephone ++49 (0)30 6392-3300

The product can be used in the residential sphere (residential sphere, business and trade sphere and small companies) and in the industrial sphere.

- Interference proof:
  EN 61000-6-2:2001
- Emitted immunity:
  EN 55022:1998
  + A1 2000
  + A2 2003, Class A

FCC Note

This equipment has been tested and found to comply with the limits for a Class A digital device, persuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.